Usman Obaid

ID# 13332

Wireless Network

Sessional Assignment- Spring 2020

Question 1: What are the latest and future trends in Wireless Networks?

Ans: Wireless tech was just an idea out on the paper when it started and now it has become one of the largest carriers of digital data all over the world. Today, this wireless technology made the functioning of several niches of industries smoother and faster.

Every enterprise, whether small or large have to depend on these wireless technologies thrive infrastructure. In coming years, wireless technology is set to include even more devices and features which would not even have been thought possible years ago.

Evolution of Wireless network-

The ability to operate devices thousands of kilometers away shows how wireless networks have evolved.

Growing demands for wireless spectrum-

Earlier, GDP of a country would tell how advanced a country is but now it's measured on how much spectrum they have access to.

5G

While the fourth generation, 4G, is still new to many nations, the telecommunication industry is already working on 5G that would be deployed soon. As this technology step towards perfection, the aim is that all devices will be wirelessly connected via 5G networks, making them commercially available worldwide. There is real and urgent demand for faster network, because of rapid and continuous growth of data traffic.

There is still more research and development needed to decide the aspects of 5G network, such as their industry regulations and technical requirements. Their needs decided include -connection speeds of up to 10 gigabits per second, and response time less than one millisecond. 5G networks will use which band of radio spectrum? And which wireless technologies are to be implemented to make this happen? These are some of the questions which are still into discussions? Makers

of this network need to know which standards they will have to comply with, including lower rates of power consumption.

IoT

As, 5G network technology will speed up the data and bring low transmission latency which will not only benefit but also exponentially boost the Internet of Things. As more devices get connected such as self-driving vehicles, smart homes, automated robots, drones, telemedicine, household appliances, underwater applications and industrial automated machines- the requirement for new network technologies will increase. Billions of dollars are invested by many companies in color sensors, microcontroller, embedded software, smart chips, and telecom services with the idea of capitalizing on the interrelationship of the Internet of Things and 5G networks.

Li-Fi (Light Fidelity)

Advancement in wireless networks is Li-Fi, or light fidelity, which uses light signals to transmit data between devices. Li-Fi provides much higher speed than Wi-Fi, reaching up to 224 gigabits per second with transmission rates of one gigabit per second. No one thought that Light bulbs could be turned into wireless routers; this was just an idea before Li-Fi devices came into existence. In coming future, smart homes will be dependent on the Li-Fi technology as it is faster and secure because light cannot penetrate through walls, the signal cannot be hacked from a remote location.

Benefits to Communication

Since, Li-Fi is suited for reaching highly sensitive areas like mines that can eliminate disrupting sensitive equipment like technology found in hospitals. Li-Fi can act as a new alternative to Wi-Fi, providing an additional option for connectivity. It can help in relieving heavy traffic from cellular as well as Wi-Fi networks and service populated areas such as concerts, shopping malls, stadiums, and sport events.

Li-Fi has shorter range but faster speed than Wi-Fi. The further away from the light source, the slower the speed. However, there is limit to the range but this would provide security in communication and help in transferring information in a better and stronger way. The area of accessibility can be limited by the users, which will indirectly help them to keep the communications secure and private.

Conclusion

The future of wireless networks seems to be faster, smarter and more efficient. As telecommunication solution providers continue to improve the technology, more people will benefit from better and more secure communication. This new network technology will also bring speed to the many smart and connected devices boosting the ever-expanding IoT. There are no specific standards raised when it comes to next generation of cellular communication (5G) but Expectations are high as estimated speeds on networks in future will range from 3.6 GBPS to over 10 GBPS which seems more challenging.

<u>Question 2:</u> You are working as a Network Specialist in ABC organization. You are asked to do research on the current and future Wireless Networks issues and challenges?

Ans: There are many Wireless networks issues and challenges. The one that we should give priority to is security. Security is the most important thing to consider when we are thinking about issues and challenges on a network, specially if they are wireless connections. Wireless connections are a lot more sensitive since all the information can be intercepted by anyone with a computer and some skills.

The first thing we should do is allow only connections with a SSL or TLS encryptions. This will allow all the data in transport to be encrypted and therefore out of the hands of hackers. We should also think about who can join the wireless network and divide the network for each organization and for guests. This way each organization will have access to the required resources only and guests would have access to basic requests only, for example an internet connection.
Finally we should use safe passwords and safe connection protocols for joining the network, as of now it is recommended WPA2 which is the safest and compatible with most devices.

Depending on the size of the organization we would probably have to consider the number of clients each router can manage and to have a network infrastructure that can be easily escalated up and escalated out.

For the future it's important to think about how many devices will be connected to the network as IoT is becoming more popular and people have more devices than ever when connecting to a network. Having a Wi-Fi 6 capable network will allow to allocate for IP addresses and serve more clients with a smaller infrastructure.

From my point of view i could figure out some of the point that raised on both current as well as future wireless network issues are:

1) Speed
now a day we are using 5G technology and as we are watching that more no of new devices will be entered inside the wireless world we have to emphasize the network bandwidth and speed through high directionality that will improve the spectrum use of signals between devices.

2) Auto recognition of devices

upcoming years more no of devices will come for that reason we have to built such technology that any new device can be recognized and its total strength
and various platform information ,device information so that network can easily identify all the aspect of that device which will enhance entire speed and routing direction based upon signal strength.

3) Concept of RFID

what could be better than this that in upcoming future when any student enter in his or her institution through RFID technology his or her presence can easily tracked wirelessly so that tracking of individual current position be possible which will be a new challenge in respect of technology optimization.

4) Software optimization and sensor compatibility

as number of devices with so many new features band signal strength it will be very hard to reach data more accurately with proper routing principle, so have to built such technique network can auto sense the path with useful information and send the packets with minimum delay and interference.

<u>Question 3:</u> Write a comprehensive note on IEEE 802.11: Wireless LAN Technology? Briefly differentiate between the standards of IEEE 802.11:

Ans: EEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands.

They are the world's most widely used wireless computer networking standards, used in most home and office networks to allow laptops, printers, and smartphones to talk to each other and access the Internet without connecting wires. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the marketplace, each revision tends to become its own standard.

The protocols are typically used in conjunction with IEEE 802.2, and are designed to interwork seamlessly with Ethernet, and are very often used to carry Internet Protocol traffic.

Although IEEE 802.11 specifications list channels that might be used, the radio frequency spectrum availability allowed varies significantly by regulatory domain.

General Description:

The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The 802.11 protocol family employs carrier-sense multiple access with collision avoidance whereby

equipment listens to a channel for other users (including non 802.11 users) before transmitting each packet.

802.11-1997 was the first wireless networking standard in the family, but 802.11b was the first widely accepted one, followed by 802.11a, 802.11g, 802.11n, and 802.11ac. Other standards in the family (c–f, h, j) are service amendments that are used to extend the current scope of the existing standard, which may also include corrections to a previous specification.[1]

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the U.S. Federal Communications Commission Rules and Regulations; 802.11n can also use that band. Because of this choice of frequency band, 802.11b/g/n equipment may occasionally suffer interference in the 2.4 GHz band from microwave ovens, cordless telephones, and Bluetooth devices etc. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively.

802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping 20 MHz-wide channels rather than the 2.4 GHz ISM frequency band offering only three non-overlapping 20 MHz-wide channels, where other adjacent channels overlap—see list of WLAN channels. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment. 802.11n can use either the 2.4 GHz or 5 GHz band; 802.11ac uses only the 5 GHz band.

The segment of the radio frequency spectrum used by 802.11 varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six of 802.11b and 802.11g fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.

In 2018, the Wi-Fi Alliance began using a consumer-friendly generation numbering scheme for the publicly used 802.11 protocols. Wi-Fi generations 1–6 refer to the 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax protocols, in that order.

There are several specifications in the 802.11 family:

- **802.11** — applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

- **802.11a** — an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11e** — a wireless draft standard that defines the ***Q****uality* ***of S****ervice* (QoS) support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.
- **802.11g** — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.
- **802.11n** — 802.11n builds upon previous 802.11 standards by adding ***m****ultiple-* ***i****nput* ***m****ultiple-****o****utput* (MIMO). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g.
- **802.11ac** — 802.11ac builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three stream) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beamforming capabilities by default to help achieve its higher wireless speeds.
- **802.11ac Wave 2** — 802.11ac Wave 2 is an update for the original 802.11ac spec that uses MU-MIMO technology and other advancements to help increase theoretical maximum wireless speeds for the spec to 6.93 Gbps.
- **802.11ad** — 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specs, with a theoretical maximum transfer rate of up to 7Gbps (Gigabits per second).
- **802.11ah**— Also known as Wi-Fi HaLow, 802.11ah is the first Wi-Fi specification to operate in frequency bands below one gigahertz (900 MHz), and it has a range of nearly twice that of other Wi-Fi technologies. It's also able to penetrate walls and other barriers considerably better than previous Wi-Fi standards.

- **802.11r** - 802.11r, also called *Fast **B**asic **S**ervice **S**et* (BSS) Transition, supports VoWi-Fi handoff between access points to enable VoIP roaming on a Wi-Fi network with 802.1X authentication.
- **802.1X** — Not to be confused with 802.11x (which is the term used to describe the family of 802.11 standards) 802.1X is an IEEE standard for port-based Network Access Control that allows network administrators to restricted use of IEEE 802 LAN service access points to secure communication between authenticated and authorized devices.