Wi-Fi: Current Technology, Challenges and Future Directions

Parveen Kumar
Assistant Professor, SPN College Mukerian
parveenspn20@gmail.com

***Abstract*— Wireless Networking has changed the way people communicate and share information by eliminating the boundaries of distance and location. Although Wireless Networking is regarded as Networking Future but still there are some unsolved issues which is preventing the wide adaption of Wireless Technologies. In this paper we have tried to discusses latest wireless technologies: Wi-Fi. The objective in this paper is to briefly describe the technology as well as the benefits and risks involved in their implementation.**

***Keywords*— Wifi, Super WiFi, Wimex, HetNets, IEEE802.11 x standards, Cognitive WiFi, WiGig**

I. INTRODUCTION

Wi-Fi[1]is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked phrase that means IEEE 802.11x. The use of wireless technology is quickly becoming the most popular way to connect to a network. Wi-Fi is one of the many available technologies that offer us the convenience of mobile computing. The thought of working anywhere and sending data to and from a device without physical connection is becoming increasingly attractive for many consumers and businesses.

WiFi is a technology that uses radio waves to provide network connectivity. A WiFi connection is established using a wireless adapter to create hotspots - areas in the vicinity of a wireless router that are connected to the network and allow users to access internet services. Once configured, WiFi provides wireless connectivity to your devices by emitting frequencies between 2.4GHz - 5GHz, based on the amount of data on the network. WiFi is a universal wireless networking technology that utilizes radio frequencies to transfer data. WiFi allows high-speed Internet connections without the use of cables.

The term WiFi is a contraction of "wireless fidelity" and commonly used to refer to wireless networking technology. The WiFi Alliance claims rights in its uses as a certification mark for equipment certified to 802.11x standards. WiFi is a freedom – freedom from wires. It allows you to connect to the Internet from just about anywhere — a coffee shop, a hotel room, or a conference room at work. What's more – it is almost 10 times faster than a regular dial-up connection. WiFi networks operate in the unlicensed 2.4 radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate, respectively. To access WiFi, you need WiFi enabled devices (laptops or PDAs). These devices can send and receive data wirelessly in any location equipped with WiFi access.

In 1999 a new technology called Airport was introduced by Apple Computers. The technology enabled a mobile user to establish and maintain a connection to a network without being physically linked to it by some sort of cable. This technology was then adopted and developed by the rest of the IT industry, then changed to the name we are all familiar today, Wi-Fi stands for wireless fidelity' (Dynamic Web Solutions 2007)

Wi-Fi
CORDLESS COMPUTING
WIRELESS DISPLAY

Fig1. Inter-communication of Wi-Fi

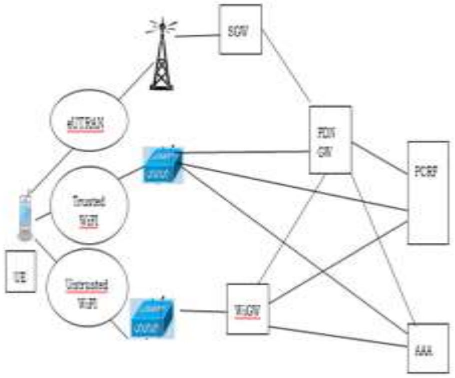

Fig2. Working of Wi-Fi

The name of a popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. The Wi-Fi Alliance [2], the organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation.

II. HOW WI-FI WORKS

WiFi works off of the same principal as other wireless devices - it uses radio frequencies to send signals between devices. The radio frequencies are completely different say from walky-talkies, car radios, cell phones, and weather radios. For example your car stereo receives frequencies in Kilohertz and Megahertz range (AM and FM stations), and WiFi transmits and receives data in the Gigahertz range.

Like mobile phones, a WiFi network [3] makes use of radio waves to transmit information across a network. The computer should include a wireless adapter that will translate data sent into a radio signal. This same signal will be transmitted, via an antenna, to a decoder known as the router. Once decoded, the data will be sent to the Internet through a wired Ethernet connection. As the wireless network works as a two-way traffic, the data received from the internet will also pass through the router to be coded into a radio signal that will be received by the computer's wireless adapter.

If you've been in an airport, coffee shop, library or hotel recently, chances are you've been right in the middle of a wireless network. Many people also use wireless networking, also called WiFi or 802.11 networking, to connect their computers at home, and some cities are trying to use the technology to provide free or low-cost Internet access to residents. In the near future, wireless networking may become so widespread that you can access the Internet just about anywhere at any time, without using wires.

III. Use of Hotspot In Wi-Fi

A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via wireless local area network (WLAN) using a router connected to an internet service provider. Public hotspots may be found in an increasing number of businesses for use of customers in many developed urban areas throughout the world, such as coffee shops. Many hotels offer wifi access to guests, either in guest rooms or in the lobby. Hotspots differ from wireless access points, which are the hardware devices used to provide a wireless network service. Private hotspots allow Internet access to a device (such as a tablet) via another device which may have data access via say a mobile device.

Internet
WiFi Hotspot
WiFi Hotspot
WiFi Hotspot
WiFi Hotspot
Restaurant

Fig3. Connection between various station with Wi-Fi

The public can use a laptop or other suitable portable device to access the wireless connection (usually Wi-Fi) provided. Of the estimated 150 million laptops, 14 million PDAs, and other emerging Wi-Fi devices sold per year for the last few years, most include the Wi-Fi feature. For venues that have broadband Internet access, offering wireless access is as simple as configuring one access point (AP), in conjunction with a router and connecting the AP to the Internet connection. A single wireless router combining these functions may suffice.

The iPass 2014 interactive map, that shows data provided by the analysts Maravedis Rethink, shows that in December 2014 there are 46,000,000 hotspots worldwide and more than 22,000,000 roamable hotspots. More than 10,900 hotspots are on trains, planes and airports (Wi-Fi in motion) and more than 8,500,000 are "branded" hotspots (retail, cafés, hotels). The region with the largest number of public hotspots is Europe, followed by North America and Asia.

IV. WiFi Frequencies[4]

A. 802.11a

The transmits at 5 GHz and can move up to 54 megabits of data per second. It also uses orthogonal frequency-division multiplexing (OFDM), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.

B. 802.11b

It is the slowest and least expensive standard. For a while, its cost made it popular, but now it's becoming less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 megabits of data per second, and it uses complementary code keying (CCK) modulation to improve speeds.

C. 802.11g

The transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.

D. 802.11n

It is the newest standard that is widely available. This standard significantly improves speed and range. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. The standard is currently in draft form -- the Institute of Electrical and Electronics Engineers (IEEE) plans to formally ratify 802.11n by the end of 2009.

V. USES OF WiFi

To connect to a Wi-Fi LAN[5], a computer has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a *station*. For all stations that share a single radio frequency communication channel, transmissions on this channel are received by all stations within range. The transmission is not guaranteed to be delivered and is therefore a best-effort delivery mechanism. A carrier wave is used to transmit the data. The data is organized in packets on an Ethernet link, referred to as "Ethernet frames"

A. Internet access

Wi-Fi technology may be used to provide Internet access to devices that are within the range of a wireless network that is connected to the Internet. The coverage of one or more interconnected access points (*hotspots*) can extend from an area as small as a few rooms to as large as many square kilometers. Coverage in the larger area may require a group of access points with overlapping coverage. For example, public outdoor Wi-Fi technology has been used successfully in wireless mesh networks in London, UK. An international example is FON.

Wi-Fi provides service in private homes, businesses, as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially, often using a captive portal webpage for access. Organizations and businesses, such as airports, hotels, and restaurants, often provide free-use hotspots to attract customers. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other buildings, provide Internet access and internetworking to all devices connected to them, wirelessly or via cable.

Similarly,[6] battery-powered routers may include a cellular Internet radio modem and Wi-Fi access point. When subscribed to a cellular data carrier, they allow nearby Wi-Fi stations to access the Internet over 2G, 3G, or 4G networks using the tethering technique. Many smart phones have a built-in capability of this sort, including those based on Android, BlackBerry, Bada, iOS (iPhone), Windo ws Phone and Symbian, though carriers often disable the feature, or charge a separate fee to enable it, especially for customers with unlimited data plans. "Internet packs" provide standalone facilities of this type as well, without use of a smartphone; examples include the MiFi- and WiBro-branded devices. Some laptops that have a cellular modem card can also act as mobile Internet Wi-Fi access points.

B. City-wide Wi-Fi

In the early 2000s, many cities around the world announced plans to construct city-wide Wi-Fi networks. There are many successful examples; in 2004, Mysore became India's first Wi-Fi-enabled city. A company called WiFiyNet has set up hotspots in Mysore, covering the complete city and a few nearby villages. In 2005, St. Cloud, Florida and Sunnyvale, California, became the first cities in the United States to offer city-wide free Wi-Fi . Minneapolis has generated $1.2 million in profit annually for its provider. In May 2010, London, UK, Mayor Boris Johnson pl dged to have London-wide Wi-Fi by 2012. Several boroughs including Westminster and Islington already had extensive outdoor Wi-Fi coverage at that point. Officials in South Korea's capital are moving to provide free Internet access at more than 10,000 locations around the city, including outdoor public spaces, major streets and densely populated residential areas. Seoul will grant leases to KT, LG Telecom and SK Telecom. The companies will invest $44 million in the project, which will be completed in 2015.

C. Campus-wide Wi-Fi

Many traditional university campuses in the developed world provide at least partial Wi-Fi coverage. Carnegie Mellon University built the first campus-wide wireless Internet network, called Wireless Andrew, at its Pittsburgh campus in 1993 before Wi-Fi branding originated. By February 1997 the CMU wifi zone was fully operational. Many universities collaborate in providing Wi-Fi access to students and staff through the eduroam international authentication infrastructure.

D. Direct computer-to-computer communications

Wi-Fi also allows communications directly from one computer to another without an access point intermediary. This is called *ad hoc* Wi-Fi transmission. This wireless ad hoc network mode has proven popular with multiplayer handheld game consoles, such as the Nintendo DS, PlayStation Portable, digital cameras, and other consumer electronics devices. Some devices can also share their Internet connection using ad hoc, becoming hotspots or "virtual routers". Similarly, the Wi-Fi Alliance promotes the specification Wi-Fi Direct for file transfers and media sharing through a new discovery- and security-methodology. Wi-Fi Direct launched in October 2010. Another mode of direct communication over Wi-Fi is Tunneled Direct Link Setup (TDLS), which enables two devices on the same Wi-Fi network to communicate directly, instead of via the access point.

VI. Architecture of Wi-Fi[7]

The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement. When two or more stations come together to communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block. A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

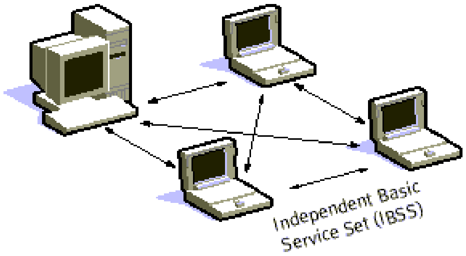

Fig3. Basic Architecture of Wi-Fi

When BSS's are interconnected the network becomes o 0ne with infrastructure. 802.11 infrastructure has several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points.

Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the Extended Service Set or ESS. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS′s transparently to the LLC.

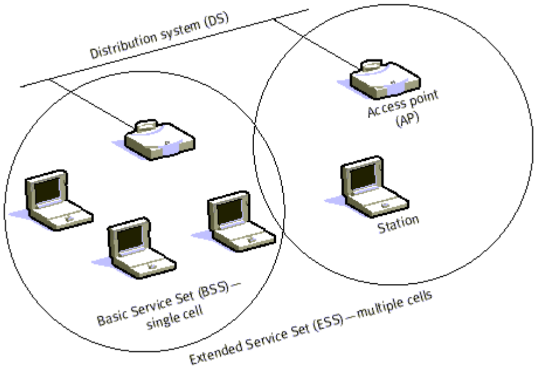
Distribution system (DS)
Access point (AP)
Station
Basic Service Set (BSS) — single cell
Extended Service Set (ESS) — multiple cells

Fig4. Infrastructure Mode

One of the requirements of IEEE 802.11[8] is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS. All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as bridge between wired and wireless. The implementation of the DS is not specified by 802.11. Therefore, a distribution system may be created from existing or new technologies. A point-to-point bridge connecting LANs in two separate buildings could become a DS.

There are two types of authentication services offered by 802.11. The first is Open System Authentication. This means that anyone who attempts to authenticate will receive authentication. The second type is Shared Key Authentication. In order to become authenticated the users must be in possession of a shared secret. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret is delivered to all stations ahead of time in some secure method (such as someone walking around and loading the secret onto each station).

Deauthentication is when either the station or AP wishes to terminate a stations authentication. When this happens the station is automatically disassociated. Privacy is an encryption algorithm, which is used so that other 802.11 users cannot eavesdrop on your LAN traffic. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) as an optional algorithm to satisfy privacy. If WEP is not used then stations are "in the clear" or "in the red", meaning that their traffic is not encrypted. Data transmitted in the clear are called plaintext. Data transmissions, which are encrypted, are called ciphertext. All stations start "in the red" until they are authenticated. MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points.

VII. Advantages of Wifi

Wi-Fi [9] eliminates the hassle and constraints of configuring a wired computer network; however, the older Ethernet technology has a few advantages over wireless networks. Wi-Fi standard revisions have pushed the technology to faster and more secure networking capabilities, which have narrowed Ethernet's advantages over wireless. Both Wi-Fi and Ethernet are operating system-independent technologies and allow any type of device that supports the related standard to connect to the network.

A. No Wires Needed

Devices that connect to a network through Wi-Fi do not need to be physically wired to the network. Setting up a Wi-Fi network can be considerably quicker and cheaper than setting up a wired network in situations where running an Ethernet cable from the network switch to the device is impractical. For example, running an Ethernet cable 30 feet across a room along a wall isn't hard to do, but running a cable up 10 feet through the ceiling can be impractical. Ethernet-based networks spanning multiple rooms and floors may need cables run through the wall.

B. Wi-Fi Device Mobility

Devices that use Wi-Fi networking are able to move anywhere within the range of the Wi-Fi access point without needing to use a wired connection. Desktop computers don't move around much, but devices like laptop computers, tablets and smart phones do. Ethernet devices need to stay connected to a cable to work, meaning the cable has to be moved with the device or the user must switch cables when relocating.

C.Data Transfer Speeds

Gigabit Ethernet, which is commonly found on non-professional grade Ethernet networking devices, is faster than every Wi-Fi standard prior to Wireless-AC. While Wireless-AC can be almost twice as fast as Gigabit Ethernet, the real-world performance speed may not be as fast. Wi-Fi uses radio technology, which is susceptible to electrical interference that can degrade signal quality and data transfer speeds. Under ideal conditions, Wi-Fi speed is theoretically superior to Ethernet, but in real-world use Ethernet may be faster.

D. Wireless Security Concerns

Without any security enabled, Ethernet [12]is more secure; however, the difference becomes negligible when an Wi-Fi network is properly secured. Any device that connects to an Ethernet network needs to be physically connected to the network. Since Wi-Fi devices can connect anywhere within range of the wireless access point, the standard is more difficult to secure than an Ethernet-based network. However, Wi-Fi networks can be adequately protected by enabling password protection and data encryption. The older WEP Wi-Fi encryption standard is practically worthless at keeping knowledgeable hackers out, but the WPA and WPA2 standards will keep even sophisticated hackers out of a network.

VIII. Disadvantages of Wifi[10]

A. Security

To combat this consideration, wireless networks may choose to utilize some of the various encryption technologies available. Some of the more commonly utilized encryption methods, however, are known to have weaknesses that a dedicated adversary can compromise**.**

B. Range

The typical range of a common 802.11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly.

C. Reliability

Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects that are beyond the control of the network administrator.

XI. Conclusion

Wi-Fi is definitely the technology of tomorrow. As technology and security undergo advancements, more people are utilizing Wi-Fi's capabilities. For personal use, families are able to use this technology so that several computers around the house can be networked together.[11] For small businesses, money is saved on expensive wiring. Larger businesses do not need to worry about how to wire large buildings and as mentioned before; employees can have more flexible work schedules. It is a sound investment because the technology will continue to get better, especially if security concerns can be curbed, which are paramount. Standards 802.11b and g are the most up and coming and a drastic increase will be seen in these standards since they are sensible and efficient for homes and small businesses. Since nearly all new laptops come with internal wireless cards, or the feature is always an option, we will see a rise in the total number of wireless LAN's being set up and hotspots will grow increasingly popular. Businesses utilizing them, such as Starbucks, have already seen the positive ramifications. Anyone interested in getting ahead with the latest and greatest technologies should invest in the technology of Wi-Fi, it is the movement of the future.

References

[1] B. Aboba, IEEE 802.1X pre-authentication, *Presentation to 802.11 WGi* (July 2002).

[2] A. Ahmad, R. Chandler, A.A. Dharmadhikari and U. Sengupta, SIMbased WLAN authentication for open platforms. Technology at Intel *Magazine* (August 2003).

[3] J. Ala-Laurila, J. Mikkonen and J. Rinnemaa, Wireless LAN access network architecture for mobile operators, IEEE Communications Magazine 39(11) (2001).

[4] G. Appenzeller, M. Roussopoulos and M. Baker, User-friendly access control for public network ports, in: *Proc. IEEE INFOCOM'99* (1999).

[5] W.A. Arbaugh, N. Shankar and J. Wang, Your 802.11 network has no clothes, in: *Proc. IEEE International Conference on Wireless LANs and Home Networks* (Dec. 2001) pp. 131–144.

[6] Aruba Networks. www.arubanetworks.com.

[7] P. Bahl, A. Balachandran, A. Miu, W. Russell, G.M. Voelker and Y.-M. Wang, PAWNs: Satisfying the need for secure ubiquitous connectivity and location services. IEEE Wireless Communications Magazine, Special Issue on Future Wireless Applications (2002) pp. 40–48.

[8] P. Bahl, A. Balachandran and S. Venkatachary, Secure wireless internet access in public places, in: *Proc. IEEE ICC'01* (June 2001) pp. 3271– 3275.

[9] P. Bahl and V. N. Padmanabhan, RADAR: An in-building RF-based user location and tracking system, in: *Proc. IEEE INFOCOM'00* (April 2000).

[10] V. Bahl, P. Bahl and R. Chandra, MultiNet: Connecting to Multiple IEEE 802.11 networks using a single wireless card, Technical Report MSR-TR-2003-46, Microsoft Research (July 2003).

[11] A. Balachandran, G.M. Voelker and P. Bahl, Hot-spot congestion relief in public-area wireless networks, in: *Proc. Workshop on Mobile Computing Systems and Applications, WMCSA'02* (June 2002) pp. 70–80.

[12] A. Balachandran, G.M. Voelker, P. Bahl and P.V. Rangan, Characterizing user behavior and network performance in a public wireless lan, in: *Proc. ACM SIGMETRICS'02* (June 2002) pp. 195–205.