Past, Present, and Future 802.11 WiFi Standards and Technologies

Abstract:

This paper contains an exploration of how Wireless Fidelity (WiFi), or 802.11 standards, have changed over the years. It reviews the different technologies and procedures that have been implemented, such as data encoding, bandwidth modulation, encryption, data integrity preservation, and special streaming. It also addresses the benefits and costs associated with current and future generation standards. Included in the discussion are the original 802.11 standard released in 1997, the current 802.11ac and 802.11ad standards, and future standards such as 802.11ax and 802.11ay.

Introduction:

An integral part of modern life is everyone’s ability to communicate wirelessly on demand. Wireless communication is facilitated by Wireless Local Area Networks (WLANs), also known as WiFi networks, the many interconnected networks through which our mobile devices, laptops, and even desktops communicate and access the Internet. WiFi has had dramatic impact on how computers have been used over the years; it enabled the revolution of mobile devices and laptops. Because WiFi networks can coexist with the existing Ethernet (or wired) networks and copper cabling of Internet Service Providers (ISPs), it has become increasingly ubiquitous over the years, with consumers expecting WiFi on demand, anywhere, anytime.

Characteristics of WiFi Networks:

The basic characteristics of WiFi networks are simple. They are similar to the Ethernet networks described by the IEEE 802.3 standard. The basic unit of networking is a single WiFi network consisting of stations, or wireless clients, and an Access Point (AP). This is called a Basic Service Set (BSS). However, a WiFi network does not require a central access point—called an ad-hoc network, or an Independent Basic Service Set (IBSS)—where each station relays communications to all others [5]. While local networks are useful in transferring data between stations in the same general location, many of these BSS’s can be connected through cabling to create larger scale networks—such as the Internet. The Extended Service Set (ESS) is the network of access points. The connections between the access points are called the Distribution Service (DS) and are usually provided by ISPs. Finally, stations themselves are transparent to the DS, as it only sees access points. The access points communicate with one another and coordinate their connected stations [5].

Services for System Function:

There are several services that the distribution service and stations must support for the system to function correctly. First, there are the Station Services (SS), which include authentication, deauthentication, privacy, and Media Access Control (MAC) service data unit delivery. Authentication and deauthentication involves connecting and disconnecting from an AP through the use of a password. The password is encrypted using the station’s encryption service. Second, there are the Distribution System Services (DSS), on the other hand, include association, reassociation, disassociation, distribution, and integration [1]. The association services involve stations connecting and moving between AP’s, allowing the station to connect to the ESS through the AP; reassociation allows the station to move to a different AP within the same ESS;
while disassociation allows the station to leave the ESS entirely. On the other hand, distribution simply routes data from the sending AP to the receiving AP. Finally, integration allows 802.11 WiFi networks to interface with existing 802.3 wired (Ethernet) LANs [1].

**Services for Data Flow:**

Like all other technology, WiFi has drastically improved over the years through the implementation of new, faster standards. However, even with the significant improvements on speed and range, the base functionality and data link layer has not changed much since WiFi’s first iterations in the late 1990’s. The data link layer of all WiFi standards includes several services needed to smoothly direct the flow of data through the BSS. These include Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), explicit packet Acknowledgment (ACK), Request to Send/Clear to Send (RTS/CTS), and packet fragmentation [1]. CSMA/CA is similar to the protocol used in 802.3 LANs, except that over the air, a device cannot transmit and receive at the same time because the transmission would interfere with the reception. Because of this, CSMA/CA uses the second service, ACK. This means that a station, before transmitting, listens for transmissions, and if there are none, waits a random amount of time and then transmits the data. If the data arrives intact, the receiving station sends back an ACK packet. If the ACK packet is not sent or lost in transmission, the station assumes the data was corrupted and re-sends it after another random amount of time [5]. The receiving station knows if the data was correct by using an integrity check algorithm.

With the Wired Equivalent Privacy (WEP) standard, a Cyclic Redundancy Check (CRC) checksum is calculated by taking the polynomial division of the data, and is sent along with the data. Hence, if the checksum does not match the data at the receiving station, the station knows something had changed, and the data must be re-sent. However, the WiFi Protected Access 2 (WPA2) standard greatly improves the security with the use of Advanced Encryption Standard (AES) based encryption. Furthermore, for large amounts of data or data that would otherwise be costly to re-send, the second to last service is used—RTS/CTS [1]. This means that when a station wants to transmit, it sends a request to send packet, and it is relayed to every station on the network, causing them to delay all other transmissions until the current one is complete. This also solves the “hidden node” issue, where two stations cannot “hear” each other and consequently must communicate only through the AP [1]. Finally, packet fragmentation is the process of breaking down large quantities of data into smaller packets, as smaller packets are much less likely to be corrupted in transmission.
**Original 802.11 Standard:**

The original 802.11 standard, published in 1997, described a network operating in the 2.4GHz band, using data chipping and Frequency Hopping Spread Spectrum (FHSS) data transmission. This is the earliest standard, and hence most different from the current ones. FHSS split the 2.4GHz band into 75 1MHz channels, and data was split across the channels using a random hopping pattern to reduce the amount of interference from other radio waves [5]. However, in the very next standard (802.11a/b), this technology was replaced by Direct Sequence Spread Spectrum (DSSS), in which data is sent through one, much wider, channel. The original 802.11 standard specified 1 Mbps and 2 Mbps speeds, which pale by comparison to today’s standards. Even when it was first implemented, it was too slow for business applications, slowing the adoption of WLANs in general. Finally, the original 802.11 used data chipping to maintain data integrity. This meant that it would send signals in 11 bit sequences with special mathematical properties that would allow it to resolve to its intended result (either a 1 or a 0) even with significant data corruption from transmission. Each sequence was converted into a waveform and sent over the air at a rate of 1 MSp, or one million symbols per second [1].

**Evolution of Standards:**

Following the original 802.11 standard, 802.11a and 802.11b were quickly released in 1999, defining two new physical layers and data rates. 802.11b was similar to the original 802.11, except that it used a more advanced data transmission chipping, called Complementary Code Keying (CCK) [1]. This consisted of sets of 64 8-bit code words that represented variable amounts of data, which resulted in different data rates for different amounts of data loss, with a maximum rate of 11 Mbps. 802.11a operated in the 5GHz band instead of the previous 2.4GHz band, allowing for an increased number of and wider channels. Data rates increased up to 54 Mbps. 802.11a also implemented Orthogonal Frequency Division Multiplexing (OFDM), another encoding scheme that allows much higher data rates and more frequency bands [2]. OFDM is also used in modern standards. Finally, two new standards, 802.11g and 802.11n, were introduced in 2003 and 2009 respectively. 802.11g brought OFDM and comparable 54Mbps data rates to the 2.4GHz band, allowing the standard to be competitive for commercial applications. However, 802.11n replaced both 802.11a and 802.11g, as it could be operated in either the 2.4GHz or 5GHz band, and supported data rates of up to 540Mbps. Furthermore, 802.11n introduced Single-user Multiple Input Multiple Output (SU-MIMO) antennas, which, as the name implies, defined several spatial data streams [2]. Data rates were greatly increased by simply transmitting more than one stream of data. This gave rise to the AP specification of x by x. For example, a 2x2 router has two transmitting antennas and two receiving antennas, whereas a 2x1 smart TV has two transmitting antennas and one receiving antenna. However, the technology was still limited to single user connections, something that would change with the next standard [2].

**Security in WiFi:**

Data sent over WLANs was originally encrypted through the WEP algorithm. However, both modes of WEP, open system authentication and shared key authentication, had significant security issues [1]. Open System Authentication was, counter-intuitively, the more secure option, as although any station can connect to the network, it must have the correct keys to decrypt the data it receives. Shared Key Authentication, on the other hand, is handled in quite a different way—the AP sends out a challenge clear-text (non-encrypted data), which the station encrypts based on its key and sends back. The station is allowed to connect if the AP can correctly decrypt the received data. Finally, after authentication is passed, the same key is used for encrypting data. However, while this may seem more secure, it is possible to discover the key from capturing
the challenge frames sent during authentication, and once a non-authorized station has the key, it can easily decrypt data from the network because the same key is used in transmission. Because of these security issues, all 802.11 standards since 2003 have specified the much stronger 802.11i standard, more commonly known as WPA2 encryption, which supports AES encryption and per-packet keys [1]. WPA-Personal is designed for small to medium sized networks and relies on the correct key being shared with each authenticating station (basically the password). A 265 bit encryption key is generated from the passphrase using the SHA-1 hash function, using the network name (SSID) as salt [1]. Transmitted data is encrypted and integrity checked using the CCMP protocol based on the advanced encryption standard (AES). Finally, although WPA2 is much more secure than WEP, it cannot protect against weak passphrases. To protect against brute force attacks, a truly random passphrase of 20 characters is sufficient. Additionally, for added protection, the network’s SSID should not match any of the top 1000 SSIDs.

Current Standards:

Finally, the current standard, 802.11ac, was released in 2013, and the development of “Wave 2” 802.11ac is scheduled to be completed sometime in 2015. 802.11ac is also similar to the previous standard, 802.11n, except it defines a physical layer exclusively using the 5GHz band and has a much higher theoretical data rate (a maximum of about 6.2 Gbps). It is also similar to 802.11n, in that it uses the same encoding (ODFM) and the same bandwidth spectrum. However, 802.11ac also implements a new version of MIMO, Multi-User MIMO (MU-MIMO). MU-MIMO allows each special stream to be connected to a different station, effectively serving multiple users at once. To assist with the interference that would naturally occur from multiple streams connecting to different stations, the AP also utilizes beamforming, a process through which it “directs” each stream directly at the station, minimizing the amount of radiation escaping to the surroundings [3]. As with SU-MIMO, multiple streams can still be connected to the same station, increasing connection speed. A new standard, 802.11ad, although first released in 2012, is now emerging as a standard for high-bandwidth, multi-gigabit WiFi. 802.11ad operates in the relatively huge 60GHz wireless band, implementing four massive 2.16GHz channels [3]. Hence, even limited to a single data stream (802.11ad does not implement MIMO), the maximum theoretical data rate approaches 7Gbps. As with several previous standards, 802.11ad uses ODFM encoding [3].

New Standards:

There are several more standards to be released in the foreseeable future, including 802.11af, 802.11ah, 802.11ax, and 802.11ay. While not much is known about the technical specifications of each forthcoming standard, 802.11af will use TV whitespace frequencies, 802.11ah will broadcast in the 1GHz band and will have enormous range [4], 802.11ax will be an updated version of 802.11ac broadcasting in the 5GHz band, and 802.11ay will be an updated version of 802.11ad, defining a new physical layer for more efficient operation in the 60GHz band [2]. Additionally, most of these new standards will implement channel bonding, allowing multiple channels to be combined for faster data rates or increased redundancy, similar to the effects produced in a RAID array.

Open Research Challenges:

There are several challenges associated with the implementation of both 802.11ac and 802.11ad, including hardware complexity, power consumption, form factor, and manufacturing costs. First, 802.11ac hardware must implement multiple copies of RF and baseband electronics in order to support multiple data streams, and when combined with the power needed for beamforming and MIMO streams, the hardware
complexity and power needed to run 802.11ac devices is very high compared to other WiFi standards. On the other hand, 802.11ad hardware is much simpler because it only forms a single data stream. However, because of the extremely high frequency of the waves, a relatively large amount of power is needed for the waves to have large enough amplitude to be detected. To minimize the necessary amount of transmission power, 802.11ad devices use high-gain antennas and, as mentioned earlier, beamforming. Second, all antennas must be separated by at least half a wavelength (about 27mm for 802.11ac devices). While this is less of a concern for 802.11ad devices, as half a wavelength is about 2.5mm, limiting the size of 802.11ac devices can significantly decrease the amount of available antenna space. Finally, 802.11ad devices suffer from an increased cost of semiconductor manufacturing, as they must be manufactured with a 40nm manufacturing processes or smaller, while 802.11ac devices can be manufactured using more traditional, larger manufacturing processes [3].

Conclusions:

Over the years, WiFi has become requisite for daily life—in fact, it is joked that the need for good WiFi shares space with food, water, and shelter on the most basic level of Maslow’s famous hierarchy of human needs. But when WiFi goes down, even for a brief time, the “joke” seems not so far from the truth. And now, with the decline of desktop computer use and the continuing increases in wireless data rates, WiFi may soon come to dominate our business lives the way it does our personal time. What is known is that new standards such as the coming 802.11ay and 802.11ah will to continue to push up speed, reliability, and range of WLANs while driving down the cost.

List of Acronyms:

WiFi: Wireless Fidelity ...........................................................................................................................................1
WLAN: Wireless Local Area Network ......................................................................................................................1
ISP: Internet Service Provider ..................................................................................................................................1
AP: Access Point ......................................................................................................................................................1
BSS: Basic Service Set ...........................................................................................................................................1
IBSS: Independant Basic Service Set (ad-hoc network) ...............................................................................................1
ESS: Extended Service Set ........................................................................................................................................1
DS: Distribution Service ...........................................................................................................................................1
SS: Station Services ................................................................................................................................................1
MAC: Media Access Control ....................................................................................................................................1
DSS: Distribution System Services ............................................................................................................................1
CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance ......................................................................2
ACK: Acknowledgement (packet) ............................................................................................................................2
RTS/CTS: Request to Send/Clear to Send ...................................................................................................................2
WEP: Wired Equivalent Privacy

CRC: Cyclic Redundancy Check

WPA2: WiFi Protected Access 2

AES: Advanced Encryption Standard

FHSS: Frequency Hopping Spread Spectrum

DSSS: Direct Sequence Spectrum Signalling

CCK: Complementary Code Keying

ODFM: Orthogonal Frequency Division Multiplexing

SU-MIMO: Single User Multiple Input Multiple Output

MU-MIMO: Multi User Multiple Input Multiple Output

Works Cited:


