A survey of IEEE 802.11 protocols.

Chris J Arges
University of Texas
Austin,Texas,USA
christopherarges [at] gmail [dot] com

1. INTRODUCTION

Wireless networks are everywhere, from cellular telephones to connecting to the internet at your favorite cafe, the ubiquity and convenience of wireless networks makes it possible to be always connected. In particular, wireless local area networks (WLANs) provide connections for our laptops at work, at home, or at the airport. These types of wireless networks are defined today mostly by the IEEE 802.11 standard, also known as WiFi [7]. This paper will survey the landscape of the IEEE 802.11 standard, and give an overview of various amendments that are relevant to laptop and mobile users such as 802.11a,b,g,n. In addition, newer standards such as 802.11ac and 802.11ad will also be explored to give and idea of the future of these standards.

Wireless networks are vastly different than wired networks. Wireless cards have dropped in price as well as wireless access points. This means that deploying a wireless solution may be cheaper for many businesses or homes. Wired networks provide a directed medium that allows the signal to travel in a specific path, which in many cases is a point to point connection with a router. In the wireless world, the air is the medium and shared with other wireless devices. This means techniques for shared medium communications, security and propagation errors must be heavily scrutinized and developed in the standard.

The paper will look at the history of the standard, showing where, why, when, and by whom it was developed. Then, the architecture of the standard will be explored showing the various layers and how they fit into the overall networking stack. The amendments to the standard will be reviewed as well as draft amendments revealing the future of wireless technology. While it is not possible to go into every detail of this expansive protocol, this paper will try to give an overview of how these technologies all fit together. Overall, the goal of this paper is to give a look into this technology that many of us use on a daily basis.

2. 802.11 HISTORY

The history of IEEE 802.11 began with an initial standard being approved, then subsequent amendments being added to the standard as needed. This has provided a robust standard that encompasses many different speeds and frequencies as well as accommodating worldwide regional regulations. In addition to the IEEE standards, an organization called the Wi-Fi Alliance provided a way to certify that devices were interoperable and implemented the standards as defined. This allowed for ease of use an widespread adoption.

The IEEE 802.11 wireless LAN specification was initially approved during 1997. This specification included a maximum transmission rate of 1 and 2 Mb/s with frequency ranges from 2.4 to 2.4835 GHz in the United States and Europe. In addition to frequencies from 2.471 to 2.49 GHz are defined for the Japanese region. The original standard defined the basics of the MAC and PHY layers of the protocol which provide the physical and data link layers of the OSI layer model. The next amendment to this specification was called 802.11b which included maximum transmission rates of 5.5 and 11 Mb/s. This amendment was approved in 1999 and included changes to the MAC layer only. Also in 1997, 802.11a was defined which utilizes the 5 GHz band which is available in the United States. This particular amendment allows for transmission rates of 6,9,12,18,24,36,48, and 54 Mb/s. In 2003, 802.11g was approved which provided improvements in the 2.4 GHz band. It has a maximum transmission rate of 54 Mb/s and is backwards compatible with 802.11b [5]. In 2009, the 802.11n was approved as an amendment. This particular amendment provides enhancements for higher throughput up to 600 Mb/s. The prominent features include MIMO (multiple-input multiple-output) using multiple antenna, security additions, and frame aggregation [1]. In addition to these existing approved standards, 802.11ac and 802.11ad are being developed to bring gigabit speeds to wireless LANs. IEEE 802.11ad will use the 60GHz band and 802.11ac will use the 5Ghz frequencies to provide very high throughput. The amendments are scheduled to be approved at the end of 2012 [9]. Table 1 summarizes the various drafts and extensions for the 802.11 standard that have been made over the years. Overall, there have been many amendments and improvements to the standard that improve the speed of wireless transmissions. In addition to the definition of the IEEE standards, how devices are certified as compliant is also relevant to the history of wireless LANs.

In 1999 the Wi-Fi Alliance was formed to certify interoperability of WLAN devices based on IEEE 802.11. Early on, 802.11 devices had many issues operating with other vendors devices, and thus this alliance certified that the devices matched specifications and could communicate. It was originally formed as an alliance between Cisco, Conexant, Agere, Nokia, and Symbol. Currently there are almost 500 companies that have joined this alliance with new membership dues

Standard	Description	Year	Status
IEEE 802.11	WLAN; 2Mb/s; 2.4 Ghz	1997	Approved
IEEE 802.11a	WLAN; 54Mb/s; 5 Ghz	1999	Approved
IEEE 802.11b	WLAN; 11Mb/s; 2.4 Ghz	1999	Approved
IEEE 802.11g	WLAN; 54Mb/s; 2.4 Ghz	2003	Approved
IEEE 802.11n	MIMO physical layer; 600Mb/s	2009	Approved
IEEE 802.11ac	WLAN 1 Gb/s; 5GHz	Late 2012 (Est.)	Task group development
IEEE 802.11ad	WLAN 1 Gb/s; 60GHz	Late 2012 (Est.)	Task group development

Table 1: List of IEEE 802.11 Standards [5]

at a mere $15,000 [4]. In order to meet Wi-Fi certification, a device must meet core MAC/PHY interoperability for either IEEE 802.11a,b,g, or n specifications. In addition, the device must implement WPA2 wireless security as well as EAP and Protected Management Frames. The Wi-Fi Alliance also holds the trademark to Wi-Fi allowing devices to be labelled as such [4]. With these certifications, devices today enjoy ease of use, and allow us to go from work, to home, or a cafe and easily connect with the same hardware.

Historically, wireless security is also important to look at when examining IEEE 802.11. Because wireless signals broadcast across a shared medium, it is trivial to snoop all traffic generated by other wireless stations in the area. For this reason the WEP (Wired Equivalent Protocol) was developed for the original standard in 1999. The goal of this protocol was to provide security as good as a wired point-to-point connection. However, a year later weaknesses in the WEP protocol surfaced, and in 2001 a tool called 'AirSnort' was released that could automatically recover a WEP key [8]. Thus, WEP was no longer considered secure and additional standards had to be developed. In addition, open networks were still used during this initial phase. Techniques such as MAC filtering were used to introduce a sense of security, but were easily defeated by someone who can sniff authorized clients and modify their own wireless card's MAC address. In 2001 the IEEE 802.11i RSN (Robust Secure Networking) standard was being developed to address these shortfalls, however it would take some time before the standard was fully developed and accepted [6]. Because of the urgency to find a better security solution, the WiFi Alliance took early drafts of 802.11i and developed WPA (WiFi Protected Access), which was released in April of 2003. After the 802.11i RSN specification was approved, the full specification was implemented until WPA2 [3]. Currently these two standards are being using today; however some weaknesses are beginning to be discovered in WPA and WPA2 as well [8].

Wireless networks have a rich history in the development of its specification, its security, and device compliance. Because this standard has evolved it has been able to adapt and be widely adopted. Now that the history has been understood one can look at the architecture in perspective.

3. ARCHITECTURE

In this section an overview of some of the components and jargon will be reviewed. Then a brief example of how a laptop connects to a wireless network will be given. Next, an in depth look at the protocol stack and examination of the physical, MAC layers, and MAC frame format of 802.11 will be explained. First, some definitions will be explained to facilitate understanding of the WLAN specification.

3.1 Components

Many components are necessary to describe a fully wireless local area network. It is important to be able to fully understand the components before understanding how the specification defines their interactions. To facilitate understanding of various jargon, Table 2 shows a list of commonly used abbreviations and acronyms for IEEE 802.11.

The main encapsulation for wireless networks is the Basic Service Set or BSS. This includes a multiplicity of wireless devices that can connect to either each other in Ad-Hoc mode, or to an Access Point (AP) which in turn connects each of the hosts and potentially to the Internet. In Infrastructure mode, an AP is a base station that wireless clients can associate and communicate with to send and receive data. This AP can then in turn send data to a router, or in many instances have integrated routing capabilities. Typically, most home or work users of 802.11 have used Infrastructure mode. Figure 1 shows both Infrastructure (a) and Ad-Hoc (b) examples of these configurations [7].

Now a simple use-case of WLANs will be illustrated to connect the dots and give a concrete example.

3.2 Example

Because the WLAN specification is meant to cover a lot of different configurations, it is useful to imagine a single use case in order to provide a clearer picture of how this all works together. One particular example that is used frequently is connecting to a wireless network in infrastructure mode using a laptop.

For instance, imagine you have a single computer connected to a cable modem which then connects to an ISP to provide Internet access. However, your family just purchased a shiny new laptop and would also like to be able to connect to the Internet as well. One solution would be to purchase a wireless router access point, and configure it to provide wireless access to the laptop and other mobile devices, while allowing wired Ethernet connections as well. Figure 2 shows an example of how this could be set up.

One choice at this point would be deciding what type of wireless router to purchase. Currently one can buy wireless routers from a number of companies for less than $100. These routers can have multiple antennas, provide routing to wired LANs, provide different ranges of coverage, and different speeds. In particular some may be labelled as "802.11n

Abbrev.	Description
STA	Wireless Station
BSS	Basic Service Set
AP	Access Point
DS	Distribution System
MAC	Medium Access Control
BSS	Basic Service Set
IBSS	Indepdenent Basic Service Set
BSSID	Basic Service Set Identifier
SSID	Service Set Identifier
MIMO	Multiple-In Multiple-Out
QBPSK	quadrature binary phase shift keying
WLAN	wireless local area network
SIFS	Short Inter-frame Spacing
DIFS	Distributed Inter-Frame Space
FH	Frequency-Hopping spread-spectrum radio
DS	Direct Sequence spread-spectrum radio
IR	Infrared light
HR	High Rate
DSSS	direct sequence spread spectrum
OFDM	orthogonal frequency division multiplexing
CSMA/CD	carrier sense multiple access with collision avoidance
MDSU	MAC service data unit
A-MDSU	Aggregate MDSU
RA	receiver address
DA	destination address
TA	transmitter address
SA	sender address

Table 2: List of Common Acronyms Used in Describing Wireless LANs [2]

compatible", or "802.11n (draft)". Some will say WiFi certified for particular categories. As explained in the history section, WiFi certified means it has passed as set of tests to ensure interoperability with other devices. In addition, many routers will have security features such as WPA/WPA2 to ensure wireless security between stations. Many of these access points for the home user are easily configured using a web browser and a network connection to the device.

Continuing with the example, one could purchase the router and set it up like figure 2, then configure the router using a web browser with the URL set to the IP address of the router. For instance, lets say the router set its internal LAN Ethernet address to 192.168.1.1, then one could browse the URL "http://192.168.1.1" and then find the settings available here. The next step would be to enable wireless access and give it an SSID name to broadcast such as "homewifi". In addition future configuration could be completed to select appropriate channels or frequencies that may be better suited for the environment. The desktop uses a wired connection to the router, and automatically connects to the router. In turn the router connects to a cable modem, when then provides access via a coaxial cable that runs outside the house. This sounds very typical, so what happens when a laptop device actually connects?

The AP will occasionally send out beacon frames which include information about the AP's SSID and MAC address. This could be broadcast on various channels. The laptop before it connects to a wireless network then passively scans all channels for beacon frames. In addition a wireless laptop could broadcast a probe frame to be received by all APs within range, and the AP will respond to that request. Once the AP is chosen by the laptop or wireless host, the association process begins. The wireless host then sends an association request frame to the AP, and in turn the AP responds with an association response. Since the wireless host needs an IP address to do anything meaningful above the data link layer, the AP will send a DHCP discovery message and obtain an IP address for the new wireless host [7].

Now the wireless host has an IP address and can send messages to and from the AP and interact with hosts on the LAN just as any other IEEE 802 compliant device would. If the wireless host wants to communicate with a device outside the network the AP will route this traffic to a gateway such as the cable modem. Now that an example of a home network setup has been explained, what does the architecture of 802.11 look like?

3.3 Stack

The IEEE 802 family covers many different technologies for Local Area Networks (LAN). The specifications only cover the Physical and Data Link layers of the OSI model. The 802 specification itself is the overall architecture and overview. 802.1 is the specification for management of the LAN. 802.2 is the Logical Link Control (LLC) layer which provides a coherent communication layer between various MAC sublayers. 802.3 is the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) specification which is needed

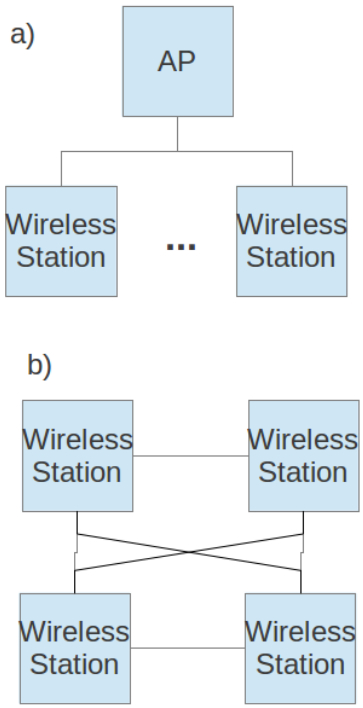

Figure 1: Infrastructure and Ad-Hoc Topologies [7]

to sort out data layer traffic on shared mediums. 802.5 is the token ring specification. Finally, 802.11 has both MAC and Physical (PHY) components which build and use other parts of the specifications. Figure 3 shows the family of specifications used by 802.11.

The IEEE 802.11 standard specifies physical and data link layers. These plug in directly to existing standards and fit nicely with our view of the Internet stack. Figure 4 gives an idea of how the various layers of IEEE 802.11 (Wireless LAN) relate to the IEEE 802 specification (Wired LAN) and the overall OSI seven layer model. This figure shows that IEEE 802.11 appears to higher layers (LLC) as a typical wired IEEE 802 LAN [2].

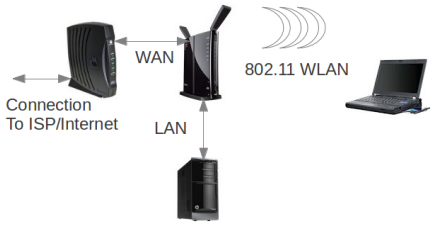

Figure 2: Typical Home Wireless Network Setup

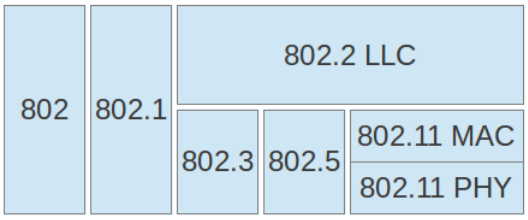

Figure 3: Related 802 Specifications [6]

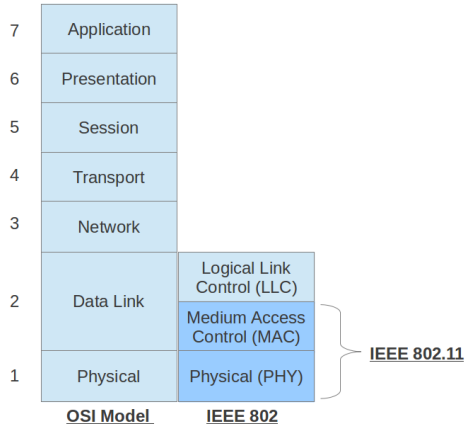

Figure 4: Architecture Compared to OSI Model [5]

Now that an overall understanding of protocol stack has been described, an examination of the 802.11 MAC layer will shed light into how this layer operates and connect into the larger stack.

3.4 Data Link Layer (MAC)

The IEEE 802.11 MAC layer provides a connection from the Physical layer to the higher layers of the Internet and 802 stack. Essentially the job of the IEEE 802.11 MAC layer is to make the wireless links look much like Ethernet to the upper levels. To accomplish such a feat a number of challenges need to be overcome that relate to the differences between wired and wireless media. The challenges include: sharing a medium, RF link quality, as well as the hidden node problem. Finally an overview of the frame format and types used by the MAC will be explained to give insight into the various parameters that are needed to send frames from station to station [6]. First the hidden node problem and RTS/CTS will be explained.

Hidden Node Problem

The hidden node problem is an issue in many wireless communication standards. Due to the nature of wireless signals it becomes very difficult for a node to detect transmissions for all the other nodes. Because wireless signals can be disrupted by obstacles and fading, sometimes a node might not be seen by all other nodes. Figure 5 shows two stations communication with one AP in the center in which the stations

cannot always detect signals from the other. This can result in unnecessary collisions because these two stations cannot see each other. One particular solution to this problem is addressed in IEEE 802.11 in the form of RTS and CTS frames. Essentially a station will send a short RTS or Request To Send frame to the AP. If no other RTS frames are transmitted and received by the AP, the AP waits the SIFS or Short Inter-frame Spacing delay and broadcasts a CTS or clear to send signal. The station that obtained the reservation can then transmit data while other stations wait. Finally after the transmission an ACK is broadcast and now the other stations are free to reserve the channel [7]. It is evident that reducing the number of collisions is vital to WLANs. Next the CSMA/CA technique will be explained.

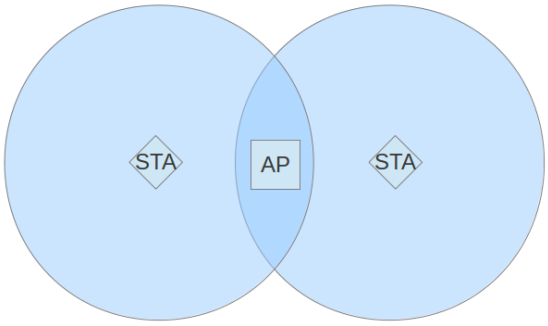

Figure 5: Hidden Node Problem Illustration [7]

CSMA/CA

Carrier sense multiple access with collision avoidance or CSMA/CD is a rather lengthy but very apt name. While Ethernet also uses CSMA it uses carrier detection rather than carrier avoidance. While this may seem subtle, it is critical to the operation of wireless internet. Carrier detection requires a station to transmit and receive at the same time which is difficult due to cost and noise. In addition because of the "hidden node problem", not all stations will be within broadcast range of any particular host; therefore collision avoidance must be used in place of collision detection. So how does CSMA/CA work?

First, if a channel is sensed to be idle, a sending station waits for a short time known as the Distributed Inter-Frame Space (DIFS). If the channel is not idle, the station chooses a random backoff value and waits for the channel to become idle. The random value is important as we could have multiple stations wanting to broadcast. This would essentially be a way to "flip a coin" to see who goes first. When the channel becomes idle the stations start counting down from their chosen values. After this backoff delay, the station starts to transmit. Then the receiving station waits for a period of time known as the SIFS or Short Inter-frame Spacing delay and if the frame passes CRC and integrity tests it sends back an ACK frame. If the receiving station gets this frame, then the receiver knows the frame was successfully sent. Otherwise the sender starts the protocol over again and tries to re-send the frame [7]. Next the various frame types will be explained.

Frame Types

Many frame types are available which are specified using the type and subtype identifier in the frame header. The main types are: management, control, and data frames. Management frames contain sub values of: association request, association response, re-association request, re-association response, probe request and response, beacons, announcement traffic indication message, disassociation, authentication and de authentication. Control frames contain subtypes of: power save poll, RTS, CTS, ACK, CF-end, and CF-end with CF-ACK. Data frames contain sub-types of: data, data with CF-ACK, data with CF-poll, data with CF-ACK and CF-Poll, null data, CF-ACK, CF-Poll, and data with CF-ACK and CF-Poll. Now that we have an overview of the types, we can examine the generic frame format.

Frame Format

Table 3 shows the fields of the 802.11 MAC layer frame. One of the most important fields is the Payload field. This contains the Layer 3 (Network layer) data to be sent and can vary between 0 and 2312 bytes depending on the MTU (Maximum Transmission Unit) being used. The Cyclic Redundancy Check (CRC) field provides a 32-bit value to allow the receiver to check for bit errors.

There are four, 6 byte (48 bit), MAC address fields provided in the WLAN MAC frame format. Because of the depth and flexibility of this standard there are many configurations in which these fields can be used. While the specification goes more in-depth on how each field is to be used, one can generalize the fields as follows. The first address is the MAC address of the wireless station that will receive the frame, which could be a wireless station or an AP. The second address is the transmitter of the frame, which again could be a wireless station or an AP. In Infrastructure mode, the third address is MAC address of the router interface, for example the AP [7]. In ad-hoc mode the addresses correspond to the absolute start and finish of a transmission, and the single hop from one station to another. By allowing for this flexibility various modes and methods can be used to describe how data should be sent from one station to another.

The sequence number, duration and frame control field are all vital to the IEEE 802.11 frame. The sequence number is used to keep track of frames and allow for acknowledgements that may get lost. The number provides a way to identify which frame was actually lost. This is critical since wireless communication can have noise issues and thus lost frames. The duration field is used when a station reserves the channel using RTS/CTS frames. The control field is a bit more complex and Table 4 shows the various bits that make up this 2 byte part of the frame. The to and from DS fields specify how the address fields should be used. The type and subtype fields distinguish the frame types [7].

3.5 Physical Layer (PHY)

In this section, the physical layer of the IEEE 802.11 standard will be explored. Wireless networks behave much differently than wired media networks. In wireless networks the medium is the air, which is shared by any wireless stations within radio communication range. This means many challenges at the physical layer must be addressed including: using a medium that does not have readily observable

Field	Frame Control	Duration	Address 1	Address 2	Address 3	Sequence Control	Address 4	Payload	CRC
Length (Bytes)	2	2	6	6	6	2	6	0-2312	4

Table 3: 802.11 Frame Format [7]

Field	Protocol Version	Type	Subtype	To AP	From AP	More frag	Retry	Power Mgt	More data	WEP	Rsvd
Length (Bits)	2	2	4	1	1	1	1	1	1	1	1

Table 4: 802.11 Frame Control Field Format [7]

boundaries, devices sharing the medium can easily transmit at the same time, unreliable communication, dynamic topologies, nodes that aren't readily visible by every node, time-varying and asymmetric propagation properties, and interference from other 802.11 wireless networks [2]. In addition to those challenges, excellent performance and adequately low power consumption are extremely important.

Various techniques have been used to communicate from one node to another. In wireless LANs, the various physical signalling techniques have evolved from amendment to amendment of the specification and may vary by location. Some of the amendments to the PHY part of the specification are because of improvements in throughput by improving or creating new signalling techniques. Because radio transmissions are controlled by various laws and regulations by country, other amendments were created to address new frequency ranges as to be available in other countries [6]. Now an examination of the various amendments to 802.11 and what PHY technologies they use or improve will be explained.

802.11

To understand some of these physical layer signalling techniques the concept of spread-spectrum signalling is critical. Spread-spectrum splits the signal into various spread-apart frequency bands, and is reconstructed at the receiver. This makes the signal less susceptible to noise, and makes it easier to achieve better performance within the constraints of regulatory requirements [6].

During the initial 802.11 draft, three types of PHY signalling were available: infra-red (IR), frequency hopping (FH), and direct sequence (DS).

One particular technology that 802.11 specifies for PHY transmission is IR or Infra-red. This uses infra-red light instead of radio waves to transmit and receive communication. However, this part of the standard has not been developed into any commercially available products [6].

Another technique is called frequency hopping (FH) also known as frequency hopping spread spectrum (FHSS). This is a spread-spectrum signalling technique that allows for a signal to transmit on a set of random frequencies from 2.4GHz to 2.5GHz in short bursts. In the original 802.11 specification this technique could achieve rates of up to 2 Mbps. Depending on the regulatory domain, a set of allowed channels between 2.4Ghz and 2.495Ghz are used. The channels are fairly narrow and between these frequencies 95 unique channels are defined. In addition to the frequencies, the hopping sequences are defined per regulatory domain. Currently FHSS is not very widely used [6].

Finally a direct sequence (DS) or direct sequence spread spectrum (DSSS) was defined which also used spread-spectrum techniques. Compared with FHSS, DSSS uses more power; however the fundamentals of DSSS can be extended to provide far better performance. The original DSSS specification provided speeds of 1 or 2 Mbps by utilizing the 2.4GHz-2.489GHz range. Within this range are fourteen 5MHz-wide channels that can be used depending on the regulatory domain. For example, in the United States and Canada channels 1 through 11 are allowed to be used.

DSSS works by 'smearing' the signal over a wide frequency band in a controlled way. Then using correlation techniques the process is inverted and the original signal is recovered. The other nice thing about this technique is that it provides some protection from interference. Much like CDMA, DSSS uses chipping streams or spreading codes to modulate or smear the data. These chipping streams are pseudo-random noise codes or PN codes which must be generated quickly to allow for proper encoding. In general a longer PN code can be used to improve the noise resilience; however, they require a codes to be generated more quickly for wider frequency bands. Figure 6 shows a diagram of how chipping codes are used at both ends to encode and recover the signal.

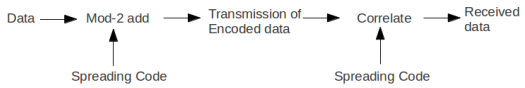

Figure 6: Using Chipping Codes [6]

These chipping codes modulate the data, but still need to be transmitted as a physical radio wave. To do this a technique called Differential Phase Shift Keying (DPSK) is used to encode the data. This works by transmitting a bit code as a particular phase shift of a waveform. For example in differential quadrature phase shift keying (DQPSK), the following symbols (bit patterns) are used: 00, 01, 11, 10. These then correspond to phase shifts of 0, 90, 180, and 270 degrees respectively. Thus, during a transmission one could shift the waveform by 270 degrees to represent the bit pat-

tern 10. While this is a very brief overview of DPSK, it is important in understanding at a high level how these bits are transmitted. Overall, DSSS is key in that it was later used in 802.11b to provide even faster rates [6].

802.11a

IEEE 802.11a introduced Orthogonal Frequency Division Multiplexing (OFDM) to the PHY specification in 1999. Hardware for this particular specification finally reached consumers around 2001. This particular part of the specification utilizes the unlicensed (in the US) 5GHz radio frequency spectrum. At its core, OFDM "encodes a single transmission into multiple sub-carriers" [6]. Each of these sub-carriers or sub-channels are multiplexed to form a faster combined channel. OFDM is much like traditional Frequency Division Multiplexing in which various frequency ranges are split up and used as parallel channels. However, the Orthogonal part of OFDM means that these channels are sufficiently split in ways that the bands don't require space between themselves to guard against interference from another transmitting channel [6]. IEEE 802.11a channels are 20 MHz wide and contain 52 sub-carriers. Within the 5Ghz range, 12 channels are available for use in the United States. The maximum 802.11a throughput ranges from 6Mbit/s all the way up to 54 Mbit/s. Besides the original specifications for the U.S. unlicensed spectrum, additional specifications were developed for use in other countries.

802.11b

High rate direct sequence (HR/DS) or high rate direct sequence spread spectrum (HR/DSSS) was defined in the 1999 802.11b amendment to the WLAN specification. It is similar to the 802.11 DSSS specification, but provides transmission rates up to 11 Mbps. Just like 802.11 DSSS, HR/DSSS also uses 11 channels above the 2.4GHz range. One major difference is that 802.11b uses complementary code keying (CCK) instead of the original chipping method used in 802.11 DS. CCK works by diving the chipping stream into 8-bit code symbols, in which some transformations to the code allow for more information to be packed into that particular symbol. Figure 7 shows a diagram of how CCK works.

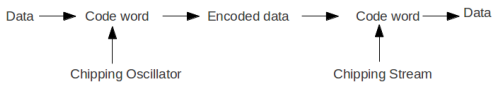

Figure 7: CCK [6]

IEEE 802.11b also uses DPSK to encode signals, but uses additional techniques to select phase angles based on if even or odd blocks are being transmitted. In addition, 802.11b also has 5.5 and 11 Mbps speeds and accordingly has different DPSK techniques for each of these modes. This particular standard brought wireless into the mainstream for home and businesses because it had a sufficient bandwidth for many tasks [6]. However, additional standards brought even better throughput and transmissions speeds.

802.11g

IEEE 802.11g standard was approved in 2003 to provide higher bit rates, but give backwards compatibility with 802.11b. There are a few physical layer specifications contained in this standard and are all prefixed with ERP or Extended Rate PHY. This includes the following physical modes: ERP-DSSS, ERP-OFDM, ERP-PBCC and DSSS-OFDM. The ERP-DSSS mode is a backwards compatible version of 802.11b providing speeds of 1, 2, 5.5, and 11 Mbps. The ERP-OFDM mode is essentially 802.11a running in the 2.4 GHz range. It supports speeds of 6,9,12,18,24,36,48, and 54 Mbps. The ERP-PBCC is an optional extension that provides 22 and 33 Mbps speeds; however it is not very widely used. DSSS-OFDM is a hybrid mode which uses DSSS to encode headers and OFDM to encode payloads of the frames. This is another optional mode that is not very widely used. Much of the specification involves in ensuring that a 802.11b device can work with 802.11g devices and vice versa. 802.11b devices will not be able to use the higher data rates, but will at least be able to communicate. Due to the backwards compatible nature of this standard the same number of channels and frequency ranges are available as 802.11b [6].

802.11n

High throughput OFDM (HT-OFDM) is defined in this standard providing up to 600 Mb/s. This standard also operates in both the 2.4 GHz and 5 GHz band using 20 Mhz band channels. In addition to 20 Mhz channels one can use 40 Mhz channels which could allow for a higher capacity channel.

In order to modulate the signal, techniques like DPSK are utilized; however in addition to phase manipulations the amplitude can also be shifted to encode additional information. Quadrature Amplitude Modulation or QAM is a method of utilizing both phase and amplitude modulation to encode the signal. 802.11n uses 16-QAM and 64-QAM encoding, which indicates the number of symbols that can be encoded into the carrier wave. These can be visualized using constellation points which show symbols on a grid where the angle from the positive x axis indicates phase and distance from origin indicates amplitude. Figure 8 shows an example of this using 16-QAM, where an amplitude is indicated by the arrow and the phase by the arch from the x-axis to the dot. Then the value of this particular point in the constellation can be decoded into a 4-bit value [1].

Another important feature of 802.11n is MIMO or Multiple-Input/Multiple-Output. This means that multiple antennas can be used by stations to simultaneously receive and transmit data. Thus, bandwidth can be greatly increased at the expense of adding more antennas. For example one can purchase a 3x3 configuration on their laptop for their laptop. This means there are 3 receiver antennas and 3 transmitter antennas. In addition to improving throughput multiple antennas can help alleviate multipath interference as well [6]. Currently this standard is becoming more widely used and most new laptops and wireless routers provide this capability. Now let's look into standards that are being currently drafted.

802.11ac / 802.11ad

The IEEE 802.11ac standard is currently being developed with an estimated approval for the end of 2012. It is being developed to be backwards compatible and coexist with 802.11a and 802.11n devices within the 5GHz band. The

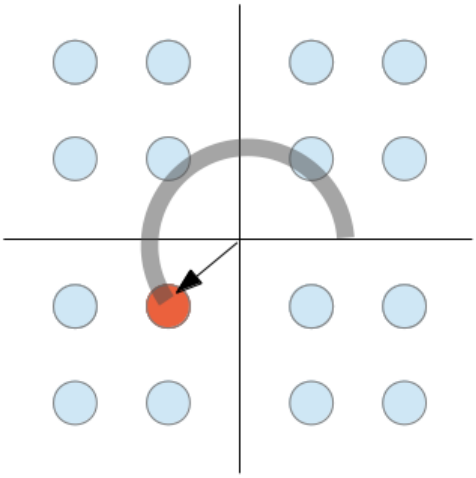

Figure 8: QAM [6] [?]

throughput goal is to achieve more than 500 Mbps throughput in at most an 80 MHz wide channel. Another goal is to achieve greater than 1 Gbps throughput with multiple devices within an 80 MHz wide channel. The use-cases for devices at this particular rate include wireless displays, HDTV, large file download, backhaul traffic, schools, and business automation.

In addition to 20 and 40 MHz wide channels, the standard will support additionally 80 and 160 MHz wide channels. Modulation will be upgraded to being capable of using 256-QAM, which means 256 encoded words within a single wave carrier. With these parameters data rates can vary from 293 Mbps up to 3.5 Gbps. Finally MU-MIMO or multiple-user MIMO is an extension to MIMO that will be available in this standard [9].

Finally 802.11ad will provide many of the same specifications as 802.11ac but within the 60 GHz band. While the range will be shorter, the throughput should support speeds of up to 7 Gb/s.

4. CONCLUSION

The entire IEEE 802.11 2012 standard is 2,793 pages; thus, this paper can only skim the surface of the depths of this standard. This paper covered the overview of why wireless LANs matter, and a history of the standard and how it has progressed from document to product. The architecture was explored examining the various components. In addition a simple use-case for a typical user was explained. The protocol stack was examined in context of the OSI model and 802 standard. Finally the MAC and PHY layers were further explored giving some depth into showing the basic operation and the various physical modes and how they have progressed over the years. It is evident that these efforts to provide a robust standard have been extremely fruitful as almost all new laptops contain this technology and many homes and public areas now have access points available. The future of the standard will be very exciting as it approaches Gigabit speeds, and continues to develop.

5. REFERENCES

[1] Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac)and physical layer (phy) specifications amendment 5: Enhancements for higher throughput. *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009)*, pages 1 –565, 29 2009.

[2] Ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pages 1 –2793, 29 2012.

[3] A. Al Tamimi. Security in wireless data networks: A survey paper.

[4] W. Alliance. The wi-fi alliance: An in-depth look. http://www.wi-fi.org/knowledge-center/articles/wi-fi-alliance-depth-look.

[5] E. Ferro and F. Potorti. Bluetooth and wi-fi wireless protocols: a survey and a comparison. *Wireless Communications, IEEE*, 12(1):12 – 26, feb. 2005.

[6] M. Gast. Wireless lan security: A short history. *Retrieved July*, 25:2005, 2005.

[7] J. Kurose and K. Ross. *Computer Networking: A Top-Down Approach*. Addison-Wesley, 2010.

[8] G. Lehembre. Wi-fi security–wep, wpa and wpa2. *Hackin9 (January 2006)*, 2005.

[9] L. Ward. 802.11ac technology introduction white paper. page 29, 2012.