Comparative Analysis of IEEE 802.11 Standards in Wireless Networking

[1]Vandana Jindal, [2]Anil Kumar Verma, [3]Seema Bawa
Thapar Univ., Patiala, Punjab, India

Abstract
Communication among devices in a network takes place according to some set of rules and procedures called protocols. Various protocols have been established by IEEE to suit the varied requirements of range, devices in the networks, cost, security and fidelity of data. .All these protocols are covered under various IEEE 802 standards which have evolved over time keeping in view the requirements described above. Among the plethora of standards, 802.11 standards governs the communication between wireless networks.

Keywords
IEEE, IEEE 802.11, BSS, IBSS, ESS, PLCP, PMD.

I. Introduction

Institute of Electrical and Electronics Engineers (IEEE) is an organization of engineers, scientists and students who are involved in developing standards for computer and electronics industry. It was founded in 1884 and came into existence as IEEE in 1963 merging American Institute of Electrical Engineers (AIEE) and Institute of Radio Engineers (IRE). These standards provide advantages like interoperability, low product cost etc. IEEE 802 standards are divided into 22 parts namely 802.3 Ethernet, 802.11 Wi-Fi, 802.15 Bluetooth/ZigBee, and 802.16 WiMax Certification etc.

Table 1: IEEE 802 Standards

IEEE 802.1	Bridging (networking) and network management
IEEE 802.2	Logical link layer
IEEE 802.3	Ethernet (CSMA/CD)
IEEE 802.4	Token bus (disbanded)
IEEE 802.5	Defines a MAC layer for a token ring (inactive)
IEEE 802.6	Metropolitan Area Networks (disbanded)
IEEE 802.7	Broadband LAN using coaxial cable (disbanded)
IEEE 802.8	Fiber optic TAG (disbanded)
IEEE 802.9	Integrated Services LAN (disbanded)
IEEE 802.10	Interoperable LAN Security (disbanded)
IEEE 802.11	Wireless LAN and mesh (Wi-Fi certification)
IEEE 802.12	Demand Priority (disbanded)
IEEE 802.13	Not used
IEEE 802.14	Cable modems (disbanded)
IEEE 802.15	Wireless PAN
IEEE 802.15.1	Blue-tooth certification
IEEE 802.15.4	ZigBee Certification
IEEE 802.16	Broadband Wireless Access (WiMax Certification)
IEEE 802.16e	(Mobile) Broadband Wireless Access
IEEE 802.17	Resilient Packet Ring
IEEE 802.18	Radio regulatory TAG
IEEE 802.19	Co-existence TAG
IEEE 802.20	Mobile Broadband Wireless Access
IEEE 802.21	Media Independent Handoff
IEEE 802.22	Wireless Regional Area Network

It comprises a family of networking standards ranging from (physical layer specifications of technologies) Ethernet to wireless. All the 802.11 specifications use the Ethernet protocol and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) for path sharing. The original modulation used in 802.11 was phase-shift keying (PSK). However, other schemes, such as complementary code keying (CCK), are used in some of the newer specifications. The newer modulation methods provide higher data speed and reduced vulnerability to interference.

II. Wireless Networking

It is a technology which allows computers to communicate amongst themselves without cables but requires certain protocols. This technology employs the IEEE 802.11 standards which provide us the technique in creating networks where network wiring is not possible.

A. Types of Wireless Networks

1. Wireless PAN

Wireless Personal Area Networks (WPANs) connect devices which are within a person's reach. It is based on IEEE 802.15 standard. The technologies used are: Bluetooth, Infrared data association, Wi-Fi.

2. Wireless LAN

Wireless Local Area Network links two or more devices over a short distance using wireless methods. It is based on IEEE 802.11 standards marketed under the name of Wi-Fi. The technologies used are spread spectrum or Orthogonal Frequency Division Multiplexing (OFDM).

3. Wireless Mesh Network

It is a wireless network made up of radio nodes arranged in a mesh topology. It consists of mesh clients (laptops/cell phones), routers and gateways. It is based on IEEE 802.11, 802.15, 802.16, cellular technologies or combinations of one or more types. More than 70 routing protocols may be used for routing the packets in a mesh network.

4. Wireless MAN

Wireless Metropolitan Area Network consists of many WLANs. It is based on IEEE 802.6 standard. The technologies used for this purpose are Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI), and Switched Multi megabit Data Service (SMDS).

5. Wireless WAN

Wireless Wide Area Network covers large areas like between cities or towns. The technologies used are LTE, WiMAX, UMTS, CDMA, cellular digital packet data (CDPD) etc. It is based on IEEE 802.16 standard.

6. Mobile Devices Network

Services rendered by the telephone dept. to phones which are mobile (not fixed)

The wireless networking hardware uses the technology that deals with radio frequencies and data transmission. The most widely used standard is 802.11 given by IEEE. This is a standard which defines all aspects of Radio Frequency Wireless Networking.

III. Protocols

A network protocol tells us about the rules and conventions for communication to take place between network devices or specify interactions between the communicating entities. Protocols have the techniques for devices to identify and establish connections between them. They also determine how the data is to be sent and received. Wireless Application Protocol (WAP) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and instant messaging.

802.11family has a long list of over-the-air modulation techniques that use the same basic protocols. 802.11 came into existence in 1997. It is thus said to be the first wireless networking standard. After this, many standards came into existence like 802.11b, 802.11g, and 802.11n etc. Of all these, 802.11b was the first most widely accepted standard followed by others. The standards (c-f, h, j) are actually the service amendments and extensions or corrections to the previous specifications.

A. 802.11-1997 (802.11 legacy)

IEEE 802.11 (legacy mode) [1, 3, 4, 5, 6] is actually the original version of the IEEE 802.11 wireless networking. It used infrared rays for data transmission at the speed of 1-2 Mbps. It also employed frequency hopping or direct-sequence spread spectrum (DSSS). DSSS version of legacy 802.11was quickly replaced by 802.11b amendment in 1999 whose transfer rate rose up to 11Mbps.The 802.11 architecture resides in the Data Link Media Access Control (MAC) sub layer and the physical layer in the OSI reference model. It is the original version of IEEE 802.11 wireless networking standard which was released in 1997, defining Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as medium access method. The technologies (physical layer) specified by this standard were:

- Diffuse infra red operating.
- Frequency hopping spread spectrum (@ 1 or 2 Mbps).
- Direct sequence spread spectrum (@ 1 or 2 Mbps).

1. IEEE 802.11 Wireless LAN Architecture

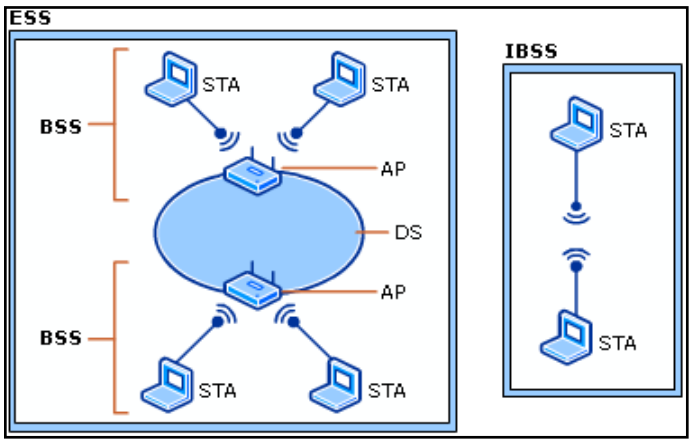


Fig. 1: Architecture of IEEE 802.11

Its architecture includes many components and services providing station mobility.

(i). Wireless LAN Station

The station (STA) is the basic component of the wireless network which may be a laptop PC, handheld device or an access point and can be either mobile or stationary. A station always supports the 802.11 protocol and a connection to the wireless media. The hardware and software of a network interface card (NIC) supports 802.11functionality.

(ii). Basic Service Set (BSS)

It has a group of many stations. The various topologies included in WLAN are:

- Independent Basic Service Set (IBSS) [1]: It is also referred to as an ad hoc network. This topology has stations connected through wireless media. In an IBSS it is not necessary that every mobile station can communicate with every other station. Only the ones which are in the close proximity (range) to each other are able to communicate amongst themselves. No relay functions are present in IBSS so the stations are required to be within range of each other.
- Infrastructure basic Service Set (IBSS): It is a BSS with an Access Point (AP).The station does not communicate directly but through the access point. All the frames are relayed between the stations by the access point.
- Distributed System: The communication takes place between two access points. The frames from the station are sent to their respective access points from where they are exchanged/forwarded to that access point having the intended station.
- Extended Coverage via an Extended Service Set (ESS): An extended service set is a set of infrastructure BSS's, where the access points communicate amongst themselves forwarding the traffic from one BSS to another, facilitating the movement of stations between BSS's. The communication amongst the access points takes place with the help of distributed system.

2. Services

802.11 standards clearly define the stations' services like – security, data delivery, de-authorization, privacy, association, disassociation, re-association, distribution and integration etc.

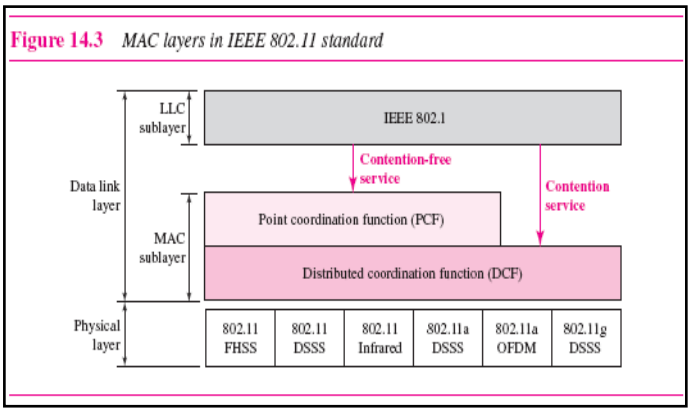


Fig. 2: MAC Layers in IEEE 802.11 Standard

(i). 802.11 Media Access Control: the following functionalities are provided

- Reliable data delivery for the upper layers over the wireless PHY media.
- Provides a controlled access method to the shared wireless media i.e. CSMA/CA.
- Provide security and privacy.

(ii). Physical Layer (PHY): The physical layer is the interface between the MAC and the wireless media where frames are transmitted and received. The PHY layer provides three different techniques for transferring of data. These are: Spread Spectrum, Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infra Red (IR).

Spread Spectrum: A technique which employs more bandwidth for reliability thus reducing the impact of interference on the media.

FHSS: A method of transmitting radio signals by rapidly switching a carrier among different frequency channels, using a pseudo random sequence known to each transmitter and receiver.

DSSS: It spreads a signal over a longer frequency band by multiplexing it with a signature code to minimize local interference and background noise.

IR: The IR PHY uses infra red light to transmit binary data using a specific modulation technique.

802.11 address mobility, security, reliability, dynamic nature of wireless LANs etc.

B. 802.11a

It is an extension of 802.11 standards. It is believed that it came into existence after 802.11b. Actually it was created at the same time but due to its high cost it made its place more in the business world rather than homes. It uses 5GHz frequency spectrum, supporting nearly 54Mbps of bandwidth. Higher the frequency, more the difficulty faced by the signals in penetrating through walls and other solid objects.

1. Architecture of 802.11a

Orthogonal Frequency Division Multiplexing (OFDM): The IEEE 802.11a standard specifies an OFDM physical layer (PHY) splitting into information across 52 different sub carriers transmitting the data at different speeds like 6, 9, 12, 18, 24, 36, 48 or 54 Mbps. It is a method that allows transmitting the high data rates over extremely hostile channels at a comparable low complexity. OFDM's spread spectrum technique distributes the data over a large number of carriers that are spread apart at precise frequencies. This spacing provides the orthogonality in this technique which prevents the demodulators from seeing frequencies other than their own. Primary goal of the OFDM PHY is to transmit MAC protocol data units (MACDUs). OFDM PHY is divided into 2 elements:

Physical layer Convergence Protocol (PLCP): The PLCP [2] sub-layer communicates with the data link layer (MAC). Its main work is to collect PLCP Service Data Units (PSDUs). The MAC layer communicates with the PLCP with certain commands through a Service Access Point (SAP). On receiving the commands the PLCP prepares MAC protocol data units (MPDUs) for transmission. The dependence of the MAC layer on the Physical Medium Dependent (PMD) sub layer is reduced by mapping MPDUs into a frame format suitable for transmission by the PMD. The PLCP also delivers incoming frames from the wireless medium to the MAC layer.

Physical Medium Dependent (PMD): The PMD sub layer provides transmission and reception of physical layer data units between two stations via the wireless medium. To provide this service, the PMD interfaces with the wireless medium and provides modulation and demodulation of the frame transmissions.

The PLCP and PMD sub layers communicate via commands through a SAP to govern transmission and reception functions.

Pros:

- Fast maximum speed.
- Less interference
- Auto configuration

Cons:

- Highest cost
- Shorter range signal so gets obstructed.

It uses OFDM based air interface. OFDM is a method of encoding digital data on multiple carrier frequencies. It is similar to coded OFDM (COFDM) and discrete multi-tone modulation (DMT) and is a frequency division multiplexing (FDM) scheme used as a digital multi-carrier modulation method.

C. 802.11b

IEEE 802.11b is an amendment to IEEE 802.11 specification. It uses CSMA/CA media access method. IEEE 802.11b is a direct extension of Direct Sequence Spread Spectrum (DSSS). It uses Complementary Code keying (CCK) as its modulation technique. CCK is a modulation scheme which helps in achieving data rate higher than 2Mbps at the expense of shorter distance.

Pros:

- Lowest cost
- Signal range good.
- Not easily obstructed.

Cons:

- Slowest maximum speed.
- Home appliances may interface on the unregulated frequency band.

D. 802.11g

The 802.11g specification is a standard for wireless local area networks (WLANs) that offers transmission over relatively short distances at up to 54 megabits per second (Mbps), compared with the 11 Mbps with the earlier 802.11b standard. Networks employing 802.11g operate at radio frequencies between 2.4GHz and 2.4835GHz, the same band as 802.11b. But the 802.11g specification employs orthogonal frequency division multiplexing (OFDM) (the modulation scheme used in 802.11a, to obtain higher data speed). This feature makes 802.11b and 802.11g devices compatible within a single network. Modification of an 802.11b access point to 802.11g compliance usually involves only a

firmware upgrade.
Pros:
- Fast maximum speed.
- Signal range is good and not easily obstructed.

Cons:
- Costs more than 802.11b
- Appliances may interfere on the unregulated signal frequency.

E. 802.11e

The wireless community faces some constraints like standards, bandwidth, link errors, power, security, mobility and roaming etc., in contrast to the wired counterparts. With increasing demand of support for real time applications like the Voice over WLAN and streaming multimedia, there is a compelling need for Quality of Service (QoS) in present day WLANs. IEEE 802.11 MAC has become a defacto standard for WLANs, but there are many inherent QoS limitations in the base standard, as it was basically developed for data services. The IEEE 802.11 Task Group E (TGe), ratified a QoS extension to the base 802.11 standard namely IEEE 802.11e. The IEEE 802.11e standard provides many mechanisms for QoS support at the MAC layer level. However, even the service differentiation provided in IEEE 802.11e is not enough to meet the QoS requirements of time bounded multimedia traffic at high load.

It 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. The amendment was incorporated into the published IEEE 802.11-2007 standard.

F. 802.11n

802.11n systems employ MIMO (multiple input, multiple output) which defines multiple transmit and receive radios – each with its own antenna – that combine to deliver multiple streams of data between stations on the same channel. By digitally controlling simultaneous transmissions and reception, 802.11n stations can effectively multiply the data rate by the number of simultaneous spatial streams they support. 802.11n defines up to 4 spatial streams. The Wi-Fi Alliance 802.11n Draft 2 certification requires that systems support at least 2 spatial streams. Spatial multiplexing can increase the burst transmission rate up to 4 times.

Pros:
- Fastest maximum speed
- Best signal range.
- More resistant to signal interference from outside sources.
- Totally backward compatible
- Many new laptops come with in-built adaptors for 802.11n and can also be added via an interface like USB.
- Features of earlier standards like Radio Management, Wireless Multi media, Intrusion Detection etc. are supposed to work better with 802.11g.

Cons:
- Standard not yet finalized.
- Costs more than 802.11g.
- Use of multiple signals may greatly interfere with nearly 802.11b/g based networks.

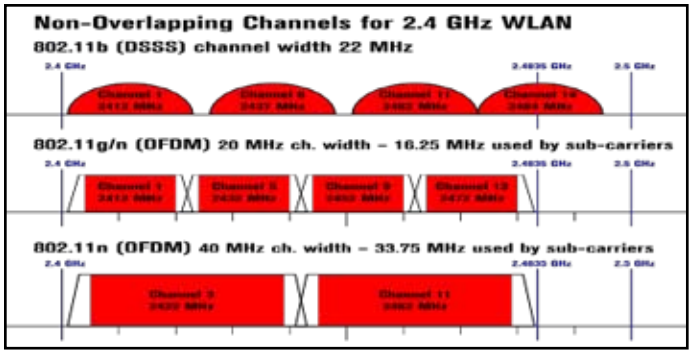


Fig. 3: Non-Overlapping Channels for 2.4 GHz WLAN

802.11b uses a DSSS and both 802.11g and 802.11a use OFDM. 802.11g clients using OFDM enjoy better performance at the same ranges as 802.11b clients do. When 802.11g clients are operating at the 802.11b rates (11, 5.5, 2, and 1Mbps), they're actually using the same modulation 802.11b does. Fig. 3 shows the 14 different channels (each 22Mhz wide) that the FCC released in the 2.4GHz range.

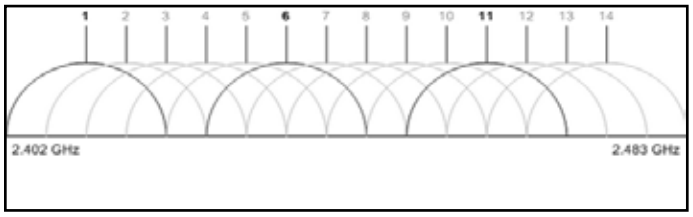


Fig. 4: 14 (each 22Mhz wide) that the FCC released in the 2.4GHz Range

IEEE 802.11 divided the 2.4GHz ISM band into 14 channels, but local regulatory agencies (FCC) designate which channels are allowed. For e.g. channels 1 through 11 in the US. Each channel in the 2.4 GHz ISM band is 22 MHz wide with 5 MHz separation, resulting in overlap with channels before or after a defined channel. Therefore, a separation of 5 channels is needed to ensure unique non overlapping channels. Given the FCC example of 11 channels, the maximum of non overlapping frequencies are channels 1, 6, and 11.

IV. Conclusion

A firm hold is required on the composition of WiFi wireless LAN technologies. Wi-Fi is designed for medium-range data transfers, and most versions of 802.11 work up to about 250-300 feet away from the access point indoors, and about 1,000 feet away outdoors and with the increase in distance between the computer/laptop and the access point, the speed and the quality deteriorates drastically. It also doesn't help when there is an interference from microwaves or cordless phones which use the same frequency that 802.11g and 802.11b use: 2.4 GHz. Another disadvantage for WiFi products is their security system. The Wired Equivalent Privacy (WEP) is the common wireless encryption standard which is easily broken even when configured accurately. To counteract this problem, however, Wi-Fi Protected Access (WPA) has been established. Many new standards are also in the pipeline like: IEEE 802.11aa, 802.11ac, 802.11ad, 802.11ae, 802.11af, 802.11ah, 802.11ai etc. The updating of the standard is the responsibility of the task group.

Table: Depicting 802 stds. & their characteristics

Standard	802.11a	802.11 b	802.11g	802.11e	802.11n
Transmission	OFDM	DSSS	DSSS/ OFDM	QoS TDMA	MIMO SDM
Spectrum (GHz)	5	2.4	2.4	2.4/ 5	2.4/5
Data Rate in Mbps	6-54	1-11	1-11 (DSSS) 6-54(OFDM)	2	100
No. of Channels overlapping	Upto 23	3	3		
Interference	HyperLAN II	Microwave, Cordless Phones,Bluetooth, HomeRF, Light Bulbs!			
Security	WEP/WPA	WEP/WPA	WEP/WPA		
Basics of physical and logical networking concepts	Specifies a PHY that operates in the 5 GHz U-NII band in the US - initially 5.15-5.35 AND 5.725-5.85 - since expanded to additional frequencies, Uses Orthogonal FDM, Enhanced data speed to 54 Mbps, Ratified after 802.11b	Enhancement to 802.11 that added higher data rate modes to the DSSS (Direct Sequence Spread Spectrum) already defined in the original 802.11 standard, Boosted data speed to 11 Mbps, 22 MHz Bandwidth yields 3 non-overlaping channels in the frequency range of 2.400 - 2.4835 GHz, Beacons at 1 Mbps, falls back to 5.5, 2, or 1 Mbps from 11 Mbps max.	Extends the maximum data rate of WLAN devices that operate in the 2.4 GHz band, in a fashion that permits interoperation with 802.11b devices, Uses OFDM, Operates at up to 54 megabits per second (Mbps), with fall-back speeds that include the “b” speeds.	Enhancement to 802.11 that includes quality of service (QoS) features, Facilitates prioritization of data, voice, and video transmissions	Higher-speed standards -- under development, Several competing and non-compatible technologies; often called “pre-n”, Top speeds claimed of 108, 240, and 350+ MHz, Competing proposals come from the groups, EWC, TGn Sync, and WWiSE and are all variations based MIMO.

References

[1] IEEE 802.11 Working Group (1997-11-18). IEEE 802.11-1997, Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications.

[2] [Online] Available: http://www.media.techtarget.com

[3] "Official IEEE 802.11 working group project timelines”, Sept. 19, 2009

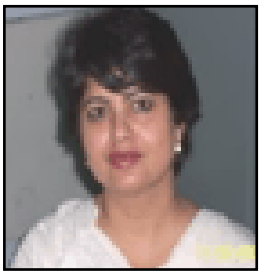
[4] "Wi-Fi CERTIFIED n: longer-Range, Faster Throughput, Multimedia-Grade Wi-Fi networks”, September 2009.

[5] "802.11n Delivers Better Range”, Wi-Fi Planet, 2007-05-31

[6] IEEE 802.11 Working Group (1997-07-15). IEEE 802.11-1999, Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications.

Vandana Jindal, B.Tech, MCA, M.Phil. is an Assistant Professor and Head of Department of Computer Science at D.A.V College, Bathinda and a Doctoral student in the Department of Computer Science, Thapar University, Patiala. Since January 2009, she has been associated with Thapar University and has been working on Wireless Sensor Networks. Apart from WSNs, her research interests include Database Management Systems. She is a member of IEEE and IEI.

A K Verma is currently working as Assistant Professor in the department of Computer Science and Engineering at Thapar University, Patiala in Punjab (INDIA). He received his B.S. and M.S. in 1991 and 2001 respectively, majoring in Computer Science and Engineering. He has worked as Lecturer at M.M.M. Engg. College,Gorakhpur from 1991 to 1996. From 1996 he is associated with the Thapar University. He has been a visiting faculty to many institutions. He has published over 100 papers in referred journals and conferences (India and Abroad). He is member of various program committees for different International/National Conferences and is on the review board of various journals. He is a senior member (ACM), MIEEE, LMCSI (Mumbai), GMAIMA (New Delhi). He is a certified software quality auditor by MoCIT, Govt. of India. His main areas of interests are: Bioinformatics, database management systems and Computer Networks. His research interests include wireless networks, routing algorithms, securing ad hoc networks and design/develop applications for other fields based on IT.



Seema Bawa holds M.Tech (Computer Science) degree from IIT Kharagpur and Ph.D. from Thapar Institute of Engineering & Technology, Patiala. She is currently Professor and Dean of Students' affairs (DOSA). Her areas of interest include Parallel and distributed computing, Grid computing, VLSI Testing and network management. Prof. Bawa is member of IEEE, ACM, Computer society of India and VLSI Society of India.