Wi-Fi Communication

Theory

Wireless Fidelity (Wi-Fi) is a name for wireless communication technology based on IEEE 802.11 standards. Due to its mass deployment, Wi-Fi is almost synonymous with Wireless Local Area Networks (WLAN). The IEEE 802.11 is a part of the IEEE 802 set of network protocols and specifies a set of Medium Access Control (MAC) and Physical Layer (PHY) protocols for WLAN. The first IEEE 802.11 standard was released in 1997 and was named IEEE 802.11-1997. This standard specifies communication in the 2.4 GHz band with a maximal data rate of 2 Mb/s on the PHY. At the beginning of the standardization, devices communicating via IEEE 802.11-1997 suffered from incompatibility issues. In 1999, standards IEEE 802.11a and IEEE 802.11b were released. The IEEE 802.11a specifies communication in the 5 GHz bands with a maximal data rate of 54 Mb/s, whereas the IEEE 802.11b specifies communication in the 2.4 GHz band with a maximal data rate of 11 Mb/s. The most significant expansion of Wi-Fi came with the introduction of the IEEE 802.11g standard in 2003, specifying communication in the 2.4 GHz band with a maximal data rate of 54 Mb/s.

The second significant improvement in Wi-Fi communication arrived in 2009 with standard IEEE 802.11n, specifying communication in both 2.4 and 5 GHz bands and a maximal data rate of 600 Mb/s. The improvement in maximal data rate was achieved via the merge of multiple communication channels and, most importantly, the exploitation of the Multiple-Input and Multiple-Output (MIMO) communication method enabling concurrent use of up to 4 parallel communication paths at once. Due to the increased computing requirements on routers with MIMO, several devices labeled IEEE 802.11n-lite compliant with IEEE 802.11n but without MIMO were introduced. The maximal data rate of devices with IEEE 802.11n-lite is 150 Mb/s with 40 MHz bandwidth.

The third significant improvement was standardized under IEEE 802.11ac in 2013. Communication is done only in the 5GHz band, with bandwidth up to 160 MHz, modulation up to 256 Quadrature Amplitude Modulation (QAM), and 8x8 MIMO. The maximal data rate with total bandwidth (160 MHz), the best modulation (256 QAM), and the highest MIMO (8x8) are up to 6,77 Gb/s.

Due to the ever-increasing requirements on wireless communication, standard IEEE 802.11ax is already in the progress of standardization, with an expected release in 2020. The IEEE 802.11ax exploits Orthogonal Frequency Division Multiple Access (OFDMA) instead of Orthogonal Frequency Division Multiplex (OFDM) to increase transmission efficiency. Furthermore, it supports up to 1024 QAM, operates in both 2.4 and 5 GHz bands, and enables up to 8 Multi-User MIMO (MU-MIMO) streams, compared to 4 MU-MIMO streams for IEEE 802.11ac.

The IEEE 802.11 standards also define communication in 60 GHz bands, also known as WiGig, for short-distance communication with high data rates up to 6.7 Gbit/s, for example, for transmission of ultra-high-definition video streams.

Due to the high number of standards in IEEE 802.11, it became clear to the Wi-Fi alliance that it is hard to orient in the standards and, thus, starting with IEEE 802.11n, a Wi-Fi generation system was introduced. So, IEEE 802.11n is Wi-Fi 4, IEEE 802.11ac is Wi-Fi 5, and so on, as shown in Table 1. The maximal data rate of Wi-Fi depends on the selected IEEE 802.11 standard, which is supported by both sides of the communication link, i.e., Access Point (AP) and receiver (smartphone, notebook, etc.). Today, most of the communication exploits IEEE 802.11n or even IEEE 802.11ac. However, due to lower costs and requirements, many devices still support only IEEE 802.11b or IEEE 802.11g. Modifying the

communication data rate by selecting communication bandwidth and the 2.4 or 5 GHz band is possible based on the chosen standard.

On the other hand, clients (devices connected to APs) must support the same standards and configuration. For example, communication will not be possible if the Wi-Fi AP operates in 5 GHz, which has wider bandwidth and suffers less interference, but the client supports only the 2.4 GHz band. The same happens for standards, e.g., AP using IEEE 802.11n but client supporting only up to IEEE 802.11g. Thus, it is best to select the configuration supported by all clients or use multiple configurations to support even the worst client.

It should be noted that the maximal data rates of given standards are only theoretical, and actual data rates are lower (approximately half). This is because these maximal data rates are for PHY, and apart from user data, redundant and service information is also being transmitted. Furthermore, channel quality degrades due to signal propagation and interference from other devices. The primary cause of lower data rate is caused by a high number of connected clients, which must share the same bandwidth in the same manner as Ethernet, on which WLAN is based and accordingly modified.

Table 1. Wi-Fi standards[1].

Standard	Generation	Release year	Frequency band [GHz]	Maximal bandwidth [MHz]	Maximal data rate [Mb/s]
IEEE 802.11	-	1997	2.4	22	2
IEEE 802.11b	Wi-Fi 1	1999	2.4	22	11
IEEE 802.11a	Wi-Fi 2	1999	5	20	54
IEEE 802.11g	Wi-Fi 3	2003	2.4	20	54
IEEE 802.11n	Wi-Fi 4	2009	2.4/5	40	600
IEEE 802.11ac	Wi-Fi 5	2013	5	160	6770
IEEE 802.11ax	Wi-Fi 6	2020	2.4/5	160	9608
	Wi-Fi 6E		2.4/5/6		
IEEE 802.11ah	HaLow	2017	0.9	16	347
IEEE 802.11ad	WiGig	2012	60	2160	7000
IEEE 802.11	Wi-Fi 7	2024	2.4/5/6	320	46120

Communication frequencies and transmission power

Wi-Fi communication exploits frequency channels in bands 2.4 GHz a 5 GHz. Both 2.4 and 5 GHz bands are unlicensed; thus, other wireless communication can occur in these bands, such as Bluetooth (IEEE 802.15.1) or ZigBee (IEEE 802.15.4). The only limitation on these bands is the maximal transmission power defined by the Equivalent Isotropic Radiated Power (EIRP).

The 2.4 GHz band contains 14 frequency channels with center frequencies from 2.412 GHz to 2.484 GHz, where central frequencies are separated by 5 MHz, apart from the separation between the 13th and the 14th channels with a separation of 12 MHz. The range of useable channels depends on the region where the Wi-Fi is deployed. Each of the 14 channels in the 2.4 GHz band can be legally exploited in Japan, whereas in Europe and most of the world (excluding the USA with 11 and Canada with 12), only the first 13 channels (up to 2.472 GHz) can be exploited. The Wi-Fi in the 2.4 GHz bands can operate with 20 to 40 MHz bandwidth (based on specification); thus, the frequency channels overlap. Therefore, in the Czech Republic (CZ), in the 2.4 GHz band, only 4 Wi-Fi networks (assuming IEEE 802.11n) can be deployed simultaneously without overlapping and, thus, interfering. The maximum EIRP for the 2.4 GHz band is 100 mW (20 dBm).

[1] http://www.wi-fi.org/discover-wi-fi/15-years-of-wi-fi

These disadvantages of the limited number of frequency channels and channel overlapping are partially solved in the 5 GHz bands. The 5 GHz band in Europe is between 5.150 GHz and 5.825 GHz, with 24 frequency channels and a separation of 20 MHz. These channels are further divided into three bands:

- RLAN band 1 (5150 – 5350 MHz)
  - sub-band I (5150 – 5250 MHz)
    - Band for indoor using
    - EIRP = **200 mW (23 dBm)**
  - sub-band II (5250 – 5350 MHz)
    - Band for indoor using
    - EIRP = **200 mW (23 dBm)**
- RLAN band 2 (5470 – 5725 MHz)
  - Band for indoor and outdoor using
  - EIRP = **1000 mW (30 dBm)**
- RLAN band 2 (5725 – 5875 MHz)
  - Band for indoor using
  - EIRP = **25 mW (14 dBm)**

Furthermore, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) must be used in all sub-bands, or the EIRP must be reduced to half the maximum value. These features are necessary for cooperation Wi-Fi technology with other radio systems in the same bands, typically meteorologic radars.

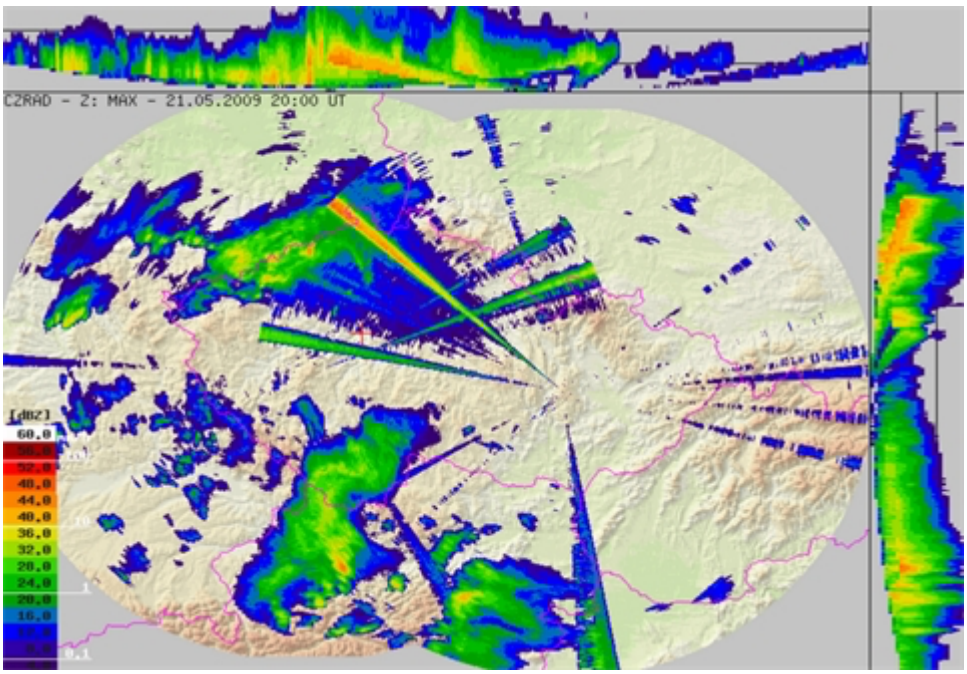


Fig. 1: Meteorologic radar interferes with Wi-Fi signals in the 5 GHz band.

Exceeding maximal transmission power can lead not only to introducing severe interference to other communication links but, if found by the local regulator, can be punished by penalization. Furthermore, if interference from other transmitters within transmission power limits is found, providers should work it out themselves, for example, by reducing transmission power or selecting a different channel.

However, if an agreement is not reached, the regulator follows the law, and the provider who started using the spectrum in disagreement must stop communicating.

Wi-Fi Network Signal Parameters

For best performance in a wireless environment, it is critical that wireless devices can distinguish received signals as legitimate information they should be listening to and ignore any background signals on the spectrum. A concept known as the Signal Noise Ratio, or **SNR**, ensures the best wireless functionality. The SNR differs between the received wireless signal (**RSSI** - Received Signal Strength Indication) and the noise floor. The noise floor is the sum of noisy background transmissions that are emitted from either other devices that are too far away for the signal to be intelligible or by devices that inadvertently create interference on the same frequency.

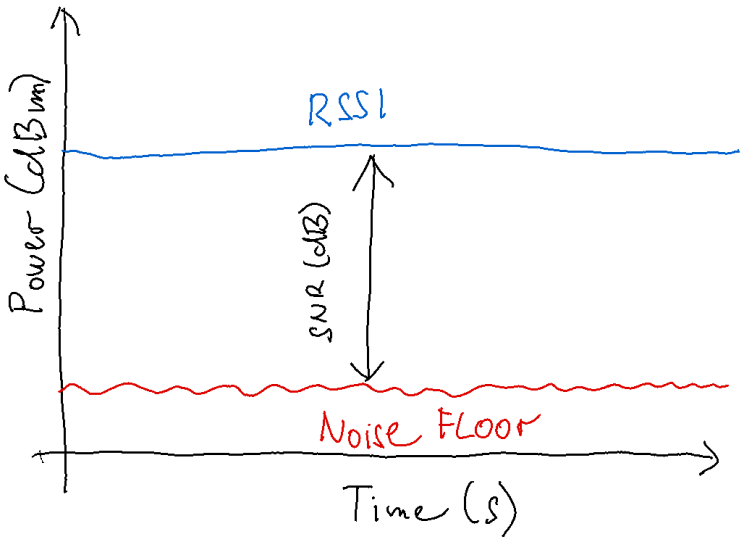


Fig. 2: SNR vs. RSSI vs. Noise Flow.

The further a received signal is from the noise floor, the better the signal quality. Signals close to the noise floor can be subject to data corruption, resulting in retransmissions between the transmitter and receiver. This will degrade wireless throughput and latency as the retransmitted signals take up airtime in the wireless environment.

Another parameter that can be monitored for Wi-Fi devices is Client Connection Quality (CCQ). Values are %. CCQ is a value in percent that shows how effective the bandwidth is used regarding the theoretically maximum available bandwidth. CCQ is a weighted average of values T_{min}/T_{real} that get calculated for every transmitted frame, where T_{min} is the time it would take to transfer a given frame at the highest rate with no retries, and T_{real} is the time it took to transmit the frame in real life (considering necessary retries it took to transmit frame and transmit rate).

Only Channel State Information[2] (CSI) data will provide a comprehensive view of Wi-Fi communication. CSI has been introduced in the IEEE 802.11n standard and describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, for example, scattering, fading, and

[2] https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/wifi.html#wi-fi-channel-state-information

power decay with distance. The method is called channel estimation. The CSI makes it possible to adapt transmissions to current channel conditions, which is crucial for achieving reliable communication with high data rates in multiantenna systems. Complex signal analysis[3] can be performed using CSI data. For example, motion detection of people/objects moving in a room with a Wi-Fi AP may be performed, as shown in many publications.

Every reasonable Wi-Fi device manufacturer specifies the required receive sensitivity (RSSI) for a given modulation in the device's product datasheet. If the antennas of the communicating devices have free space between them, it is straightforward to derive the required transmit power. This should not exceed the limits that are defined for the given area.

Sensitivity @PER	270M: -68dBm@10% PER; 130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER; 1M: -90dBm@8% PER
Antenna Gain	3dBi * 3

Fig. 3: RSSI limits for Wi-Fi device TP-Link TL-WR1043ND v1.

Wi-Fi network communication chain for free space loss.

$$L_{mT} - L_{mR0} = A_T - G_T + A_0 + A_R - G_R + A_{rez}$$

Where:

- L_{mT} – Power level at the transmitter output [dBm]
- L_{mR0} – Receiver sensitivity for threshold error rate [dBm]
- A_T – Attenuation of the transmission antenna lead [dB]
- G_T – Gain of the transmitting antenna [dB]
- A_0 – Free space loss attenuation → 32.4 + 20log(f*d) [dB; MHz, km]
    - d – the distance between the transmitter and the receiver
- A_R – Attenuation of the receiving antenna lead [dB]
- G_R – Gain of the receiving antenna [dB]
- A_{res} – link margin including fade margin [dB]

Practical using of this calculation can be found in the chapter Practical calculation example.

[3] https://www.sciencedirect.com/science/article/pii/S1877050921024509

Medium Access Methods

Standard IEEE 802.11 uses primary as a medium access method Carrier Sense Multiple Access with Collision[4] Avoidance (CSMA/CA). It works by checking if the channel is unoccupied for a given period, and if the channel is occupied, the transmission is suspended until the medium is free. This function is called DCF (Distributed Coordination Function). This function is used in standard Wi-Fi networks for client communication in best-effort mode.

The point coordination function (PCF) is used for AP-driven communication. PCF allows the access point as the network coordinator to manage channel access. The typical user of the PCF method is for time-critical and priority transmissions.

Problems in Wi-Fi

Hidden node problem

One of the problems of Wi-Fi is the so-called hidden node problem[5]. This problem occurs as not every client is aware of all other clients, and when this client communicates, it may be unaware of other clients communicating, thus leading to collisions. To overcome this issue, standard IEEE 802.11 defines the method Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with RTS/CTS[6] extension. These methods work by first sensing the wireless medium (given channel) and avoiding communication if another communication is ongoing via a pair of packets Request to Send / Clear to Send (RTS/CTS). Unlike regular CSMA/CA communication, if the channel is unoccupied, the client transmits RTS packed, containing information about the duration of data transmission. The receiving client replies with a CTS packet (again containing information about the duration of data transmission). Every client which receives RTS or CTS does not transmit for the duration of data transmission of the transmitting client. The correct transmission is acknowledged via ACK packet at the end of data transmission. Otherwise, transmission is repeated. These control packets reduce the maximal data rate and transmission delay, but short RTS and CTS packets significantly decrease collision probability. This feature is active on a network where bigger packets, over 2000 B, are allowed. A bigger packet leads to a higher transmission time, increasing the possibility of collision.

Traffic Jam

802.11 DCF consumes significant airtime, and 802.11 control messages usually convey very little information. For example, an ACK message can take up to 60 µs to transmit completely, which includes an amount of airtime sufficient to transmit 3240 bits at 54 Mbit/s, during which it conveys a single bit of relevant information. The following graphs illustrate the situation[7]. The problem can divide into the following parts:

- Radio interference problems → increase control frames.
- Old technology coexistence → IEEE 802.11 b and g uses different modulations → must use RTS/CTS extension to control transmission time.
- Payload type → Small packets require small frames, and small frames increase PHY overhead.

[4] https://inet.omnetpp.org/docs/showcases/wireless/hiddennode/doc/index.html
[5] https://meraki.cisco.com/blog/2017/07/the-hidden-node/
[6] https://inet.omnetpp.org/docs/showcases/wireless/hiddennode/doc/index.html
[7] http://bit.ly/WiFi6forDummies

IEEE 802.11 data rates on the physical layer (L1) are not the same as a user can measure on the upper layers (L4). They are usually half the size of the values on the physical layer.

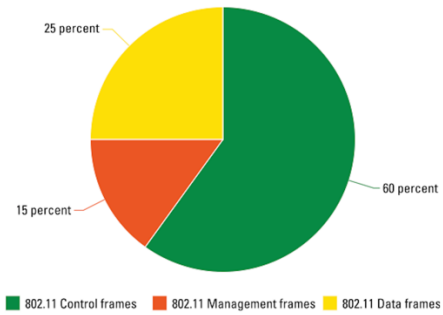


Fig. 4: Comparison of Wi-Fi frame types of occupancy.

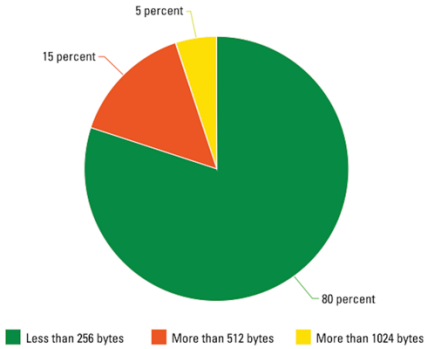


Fig. 5: Comparison of transmission effectivity of Wi-Fi packet sizes.

Exposed Node Problem

The exposed node problem occurs when a node is prevented from sending packets to other nodes because of co-channel interference with a neighboring transmitter. The situation arises in a network of multiple access points, where neighboring access points operate on the same channel but do not hear each other. If a client is between them, communicating with one of the access points, the communication of the other, actively not communicating access point, is blocked due to CSMA/CA. The latter could communicate with another client but is blocked. The solution is the use of so-called BSS Coloring (a Wi-Fi 6 feature, unique 6-bit tag in PHY header) where the following applies:

- The **same** BSS tag --> intra-BSS transmission - **not able** to transmit.
- **Different** BSS tag --> inter-BSS transmission - **able** to transmit.

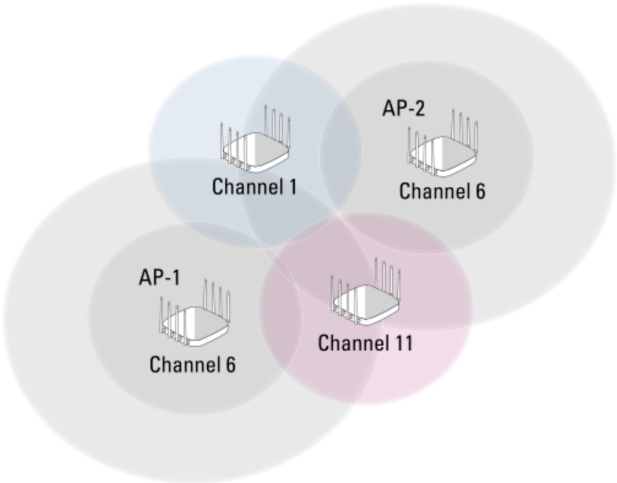
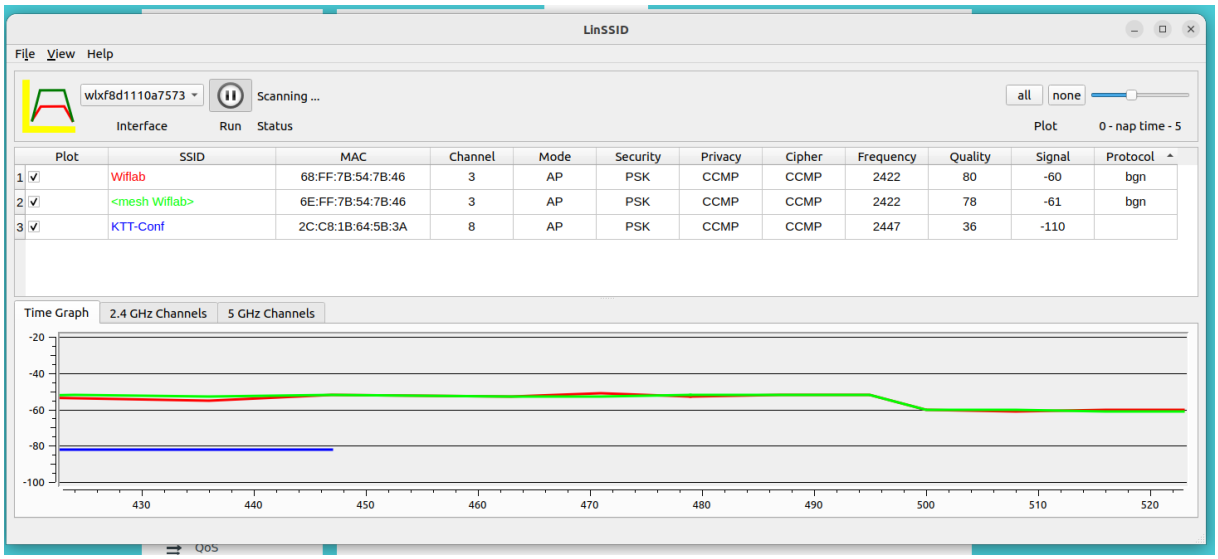


Fig. 6: Exposed node problem visualization.

Practical calculation example

Wi-Fi access point transmission power calculation from the measured signal intensity. The distance between the AP and the client device is 10 m without obstacles. The access point is TP-Link Archer C6, and the client device is the TP-Link WN821ND USB adapter.



Wi-Fi network communication chain for free space loss with L_{mT} value from LinSSID flow.

Known parameters:

- L_{mT} = ? dBm
- L_{mR0} = -53 dBm
- A_T = 0 dB
- G_T = 3 dBi
- distance = 10 m
- frequency = 2422 MHz
- A_0 = 32.4 + 20*$\log_{10}$ (frequency*distance) = 60 dB [dB; MHz, km]
- A_R = 0 dB
- G_R = -5 dBi
- A_{res} – 0 dB

$$L_{mT} = L_{mR0} + A_T - G_T + A_0 + A_R - G_R + A_{rez}$$

$$L_{mT} = -53 + 0 - 3 + 60 + 0 + 5 + 0$$

$$\underline{L_{mT} = 9\ dBm}$$

The transmit power of the access point TP-Link Archer C6 is about 9 dBm. TX Power on AP is set to LOW.