Electromagnetic interference at 2.4 GHz

From Wikipedia, the free encyclopedia

Electromagnetic interference at 2.4 GHz can affect various devices. This article details the different users of the 2.4 GHz band, how they cause interference to other users and how they are prone to interference from other users.

## Contents

1. Phone
2. Bluetooth
3. Car alarm
4. Microwave oven
5. Video devices
   - 5.1 Wi-Fi networks
   - 5.2 EIRP
6. ZigBee / IEEE 802.15.4 Wireless Data Networks
7. Resolving interference
   - 7.1 Channel change
   - 7.2 Jamming
   - 7.3 Alternative product
   - 7.4 Parameter change
   - 7.5 Adding base stations
8. See also
9. References

## Phone

Many cordless telephones and baby monitors in the United States and Canada use the 2.4 GHz frequency, the same frequency at which Wi-Fi standards 802.11b, 802.11g and 802.11n operate. This can cause a significant decrease in speed, or sometimes the total blocking of the Wi-Fi signal when a conversation on the phone takes place. There are several ways to avoid this though, some simple, and some more complicated.

- Buy/Use wired phones.
- Buy DECT 6.0 (1.9 GHz), 5.8 GHz or 900 MHz phones, commonly available today.
- Use VoIP/WiFi phones; these share the WiFi base stations and participate in the WiFi contention protocols.
- Test several different Wi-Fi channels to avoid the phone channels.

The last will sometimes not be successful, as numerous cordless phones use a feature called Digital Spread Spectrum. This technology was designed to ward off eavesdroppers, but the phone will...
change channels at random, leaving no Wi-Fi channel safe from phone interference.

**Bluetooth**

Bluetooth devices intended for use in short-range personal area networks operate from 2.4 to 2.4835 GHz. To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels up to 1600 times per second.

**Car alarm**

Certain car manufacturers use the 2.4 GHz frequency for their car alarm internal movement sensors. These devices broadcast on 2.45 GHz (between channels 8 and 9) at a strength of 500 mW. Because of channel overlap, this will cause problems for channels 6 and 11 which are commonly used default channels for Wi-Fi connections. Because the signal is transmitted as a continuous tone, it causes particular problems for Wi-Fi traffic. This can be clearly seen with spectrum analysers. These devices, due to their short range and high power, are typically not susceptible to interference from other devices on the 2.4 GHz band.

**Microwave oven**

Microwave ovens operate by emitting a very high power signal in the 2.4 GHz band. Older devices have poor shielding, and often emit a very "dirty" signal over the entire 2.4 GHz band.

This can cause considerable difficulties to Wifi and Video senders, resulting in reduced range or complete blocking of the signal.

The IEEE 802.11 committee that developed the WiFi specification conducted an extensive investigation into the interference potential of microwave ovens. A typical microwave oven uses a self-oscillating vacuum power tube called a magnetron and a high voltage power supply with a half wave rectifier (often with voltage doubling) and no DC filtering. This produces an RF pulse train with a duty cycle below 50% as the tube is completely off for half of every AC mains cycle: 8.33 ms in 60 Hz countries and 10 ms in 50 Hz countries.

This property gave rise to a WiFi "microwave oven interference robustness" mode that segments larger data frames into fragments each small enough to fit into the oven's "off" periods.

The 802.11 committee also found that although the instantaneous frequency of a microwave oven magnetron varies widely over each half AC cycle with the instantaneous supply voltage, at any instant it is relatively coherent, i.e., it occupies only a narrow bandwidth. The 802.11a/g signal is inherently robust against such interference because it uses OFDM with error correction information interleaved across the carriers; as long as only a few carriers are wiped out by strong narrow band interference, the information in them can be regenerated by the error correcting code from the carriers that do get through.

**Video devices**

Video senders typically operate using an FM carrier to carry a video signal from one room to another.
(for example, satellite TV or closed-circuit television). These devices typically operate continuously but have low (10 mW) transmit power. However, some devices, especially wireless cameras, operate with (often unauthorized) high power levels, and have high-gain antennas.\[citation needed\]

Although the transmitter of some video cameras appears to be fixed on one frequency, it has been found in several models that the cameras are actually frequency agile, and can have their frequency changed by disassembling the product and moving solder links or little switches inside the camera.

These devices are prone to interference from other 2.4 GHz devices, due to the nature of an analog video signal showing up interference very easily. A carrier:noise ratio of some 20 dB is required to give a "clean" picture.

Continuous transmissions interfere with these, causing "patterning" on the picture, sometimes a dark or light shift, or complete blocking of the signal.

Non-continuous transmissions, such as Wifi, cause horizontal noise bars to appear on the screen, and can cause "popping" or "clicking" to be heard on the sound.

**Wi-Fi networks**

Video senders can, in some areas, have very poor performance due to interference from Wi-Fi networks. Particularly in the UK, whereby most broadband providers are giving away free routers with Wireless built in and enabled by default, it is possible that no clear channel can be found for the video sender, and that it is not possible to make it work.\[citation needed\]

Video Senders are a big problem for Wi-Fi networks. Unlike Wi-Fi, they operate continuously, and also unlike Wi-Fi, are typically only 10 MHz in bandwidth. This causes a very intense signal as viewed on a spectrum analyser, and completely obliterates over half a channel. The result of this typically in a WISP type environment is that clients (who cannot hear the video sender due to the "hidden node" effect) can hear the Wi-Fi without any issues, but the receiver on the WISP's access point is completely obliterated by the video sender, so is extremely deaf. Furthermore, due to the nature of video senders, they are not interfered with by Wi-Fi easily, since the receiver and transmitter are typically located very close together, so the capture effect is very high, and Wi-Fi has a very wide spectrum, so only typically 30% of the peak power of the Wi-Fi actually affects the video sender. Also, the Wi-Fi is not continuous transmit, so it is very difficult for the Wi-Fi signal to interfere with the video sender. A combination of these factors - low power output of the Wi-Fi compared to the video sender, the fact that typically the video sender is far closer to the receiver than the Wi-Fi transmitter and the FM capture effect means that a video sender may cause problems to Wi-Fi over a wide area, but Wi-Fi causes little problems to the video sender.\[citation needed\]

802.11n WiFi networks are proving to be a source of interference for other wireless data networks operating at 2.4GHz.

**EIRP**

Many video senders on the market in the UK advertise a 100 mW equivalent isotropically radiated power (EIRP). However, the UK market only permits a 10 mW EIRP limit. These devices cause far more interference across a far wider area, due to their excessive power. Furthermore, UK video senders are required to operate across a 20 MHz bandwidth (not to be confused with 20 MHz
deviation). This means that some foreign imported video senders are not legal since they operate on a 15 MHz bandwidth or lower, which causes a higher spectral power density, increasing the interference. Furthermore, most other countries permit 100 mW EIRP for video senders, meaning a lot of video senders in the UK have excessive power outputs.\[citation needed\]

**ZigBee / IEEE 802.15.4 Wireless Data Networks**

Many ZigBee / IEEE 802.15.4-based wireless data networks operate in the 2.45–2.4835 GHz band, and so are subject to interference from other devices operating in that same band. To avoid interference from IEEE 802.11 networks, an IEEE 802.15.4 network can be configured to only use channels 15, 20, 25, and 26, avoiding frequencies used by the commonly used IEEE 802.11 channels 1, 6, and 11.

**Resolving interference**

Normally interference is not too hard to find. Products are coming onto the market cheaply which act as spectrum analyzers and use a standard USB interface into a laptop, meaning that the interference source can be fairly easily found with a little work, a directional antenna and driving around to find the interference.

**Channel change**

Often solving interference is as simple as changing the channel of the offending device. Particularly with video senders, whereby plugging in the receiver with no transmitter attached will let you "see" the neighbour's video sender, this technique is considered part of the "Installation process". Where the channel of one system, such as a Wireless ISP cannot be changed, and it is being Interfered with by something such as a video sender, the owner of the video sender is normally very happy to assist with doing this, providing it is not too much work. However the problem comes when the interference is something such as a wireless CCTV camera which is mounted on a chimney and requires a long ladder to access. Such cameras, due to their height, cause serious problems across a wide area.

**Jamming**

One cure is to jam the signal. Legally, depending on how this is done, this is acceptable. An often used method is to program an 802.11 access point on the channel used, and to set the power to maximum and the beacon interval to something like 1ms. This causes little interference to the 802.11 network, typically far less than the offending device since the 802.11 carrier sense multiple access (CSMA) mechanisms are still operational, but can cause great interference to the offending device. There are products coming on the market which are intended as 2.4 GHz jammers, intended to jam a video sender without jamming the wireless network which is receiving the interference.\[1\]

**Alternative product**

Another cure is to offer an alternative product to the owner free of charge. Typically this would be a wired camera, which normally have far better performance than wireless cameras anyway, a cable to replace the video sender, or an alternative video sender which has been hard-wired to an alternative channel, with no means of changing it back to the offending frequency.
Yet another cure is to move from 2.4GHz to another frequency which lacks the vulnerability to interference inherent at that frequency.

**Parameter change**

In extreme cases, where the interference is either deliberate or all attempts to get rid of the offending device have proved futile, it may be possible to look at changing the parameters of the network. Changing collinear antennas for high gain directional dishes normally works very well, since the narrow beam from a high gain dish will not physically "see" the interference. Often sector antenna have sharp "nulls" in their vertical pattern, so changing the tilt angle of sector antennas with a spectrum analyzer connected to monitor the strength of the interference can place the offending device within the null of the sector. High gain antennas on the transmitter end can "overpower" the interference, although their use may cause the effective radiated power (ERP) of the signal to become too high, and so their use may not be legal.

**Adding base stations**

It may seem counter intuitive, but you can reduce the interference your WiFi network causes your neighbors by adding more base stations to your own network. Every WiFi standard provides for automatic adjustment of the data rate to channel conditions; poor links (usually those spanning greater distances) automatically operate at lower speeds. Deploying additional base stations around your home or office, particularly in existing areas of poor or no coverage, reduces the average distance between a wireless device and its nearest access point and increases the average speed. The same amount of data takes less time to send, reduces channel occupancy, and gives more idle time to your neighbors. And it improves the performance of your own network.

All of the base stations in your network should be set to the same SSID (which must be different from all of your neighbors) and plugged into the same logical Ethernet segment (one or more hubs or switches directly connected without IP routers). Wireless clients then automatically select the strongest access point from all those with the specified SSID, handing off from one to another as their relative signal strengths change.

The alternative of increasing coverage by adding an RF power amplifier to a single base station usually doesn't perform as well and it can significantly increase your interference to your neighbors.

**See also**

- Electromagnetic interference

**References**


Retrieved from "http://en.wikipedia.org/wiki/Electromagnetic_interference_at_2.4_GHz"

Categories: Radio electronics

- This page was last modified on 28 October 2009 at 12:43.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.