Research Paper

Volume : 4 | Issue : 11 | November 2015 • ISSN No 2277 - 8179

Effect of Co-Channel and Adjacent Channel Interference in WIFI Networks

Engineering

KEYWORDS : WIFI Networks, Channel Interferences

S M GANESH Assistant professor, Bheema Institute of Technology and Science, Adoni

ABSTRACT

The growing technolgy of wireless devices combined with the advent of mobility applications requires in managing inference throughout their deployments. The many wireless technologies and common place electric devices already in use and newly emerging impede wireless performance.RF interference can be a major inhibitor to wireless performance, creating security vulnerabilities and wireless network instability. Among different wireless technolgies Wifi is developing very rapidly which makes the user to access the internet very faster compared to traditional technologies. In this paper we are discussing two major problems of Wifi netwroks one is co channel interference and adjacent channel interference and their realistic beliefs while deployment.

Introduction

There are number of 802.11 devices and it is true that the other same networks can cause interference with our network. This type of interference is known as co-channel and adjacent channel interference. As other 802.11 devices follow the same protocol, they tend to work cooperatively-that is, two access points on the same channel will share the channel capacity. In reality, the many other types of devices emitting in the unlicensed band dwarf the number of 802.11 devices. These devices include microwave ovens, cordless phones, Bluetooth devices, wireless video cameras, outdoor microwave links, wireless game controllers, Zigbee devices, fluorescent lights, WiMAX, and so on. Even bad electrical connections can cause broad RF spectrum emissions. These non-802.11 types of interference typically don't work cooperatively with 802.11 devices, and can cause significant loss of throughput. In addition, they can cause secondary effects such as rate back-off, in which retransmissions caused by interference trick the 802.11 devices into thinking that they should use lower data rates than appropriate. Although 802.11 protocol is designed to bovercome the problem of interference. When an 802.11 device senses an interference burst occurring before it has started its own transmission, it will hold off transmission until the interference burst is finished. If the interference burst starts in the middle of an ongoing 802.11 transmission , the lack of an acknowledgement packet will cause the transmitter to resend the packet. In the end, the packets generally get through. The result of all these hold-offs and retransmissions, however, is that the throughput and capacity of your wireless network are significantly impacted. when you deploy a dense network of access points, it's necessary to reduce the transmit signal power of each of the access points. If you don't reduce the power, the access points generate interference to each other, a phenomenon known as co-channel interference.

1 - WIFI

With the rapid development of mobile communication and the pervasive computing technology, the requirement of data service is rapidly increasing. Though traditional networks can provide accurate and reliable data services, it cannot be used effectively under indoor environment [1]. To overcome this limitation, researchers have proposed a technolgy called Wi-Fi which belongs to 802.11 family, Wi-Fi technology has attracted extensive attention because it is built upon mobile phones, which are used widely all over the world [4]. The crowded places, such as street, office buildings, shopping malls, hotels, and airports, usually have a lot of AP hot spots, which form a wide coverage of Wi-Fi network [5]. Therefore, it is feasible and practicable to adopt the Wi-Fi network and mobile phone to implement personnel positioning under indoor environments.

IEEE 802.11ac is a wireless networking standard in the 802.11 family (which is marketed under the brand name Wi-Fi), developed in the IEEE Standards Association process,[1] providing high-throughput wireless local area networks (WLANs) on the 5 GHz band. The standard was developed from 2011 through 2013 and approved in January 2014.This specification has expected multi-station WLAN throughput of at least 1 gigabit per second and a single link throughput of at least 500 megabits per second (500 Mbit/s). This is accomplished by extending the air interface concepts embraced by 802.11n: wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to eight), downlink multi-user MIMO (up to four clients), and high-density modulation (up to 256-QAM).

2 Co-Channel Interference

Co-channel interference or **CCI** is crosstalk from two different radio transmitters using the same frequency. There can be several causes of co-channel radio interference; four examples are listed here.

Cellular Mobile Networks: In cellular mobile communication (GSM & LTE Systems, for instance), frequency spectrum is a precious resource which is divided into non-overlapping spectrum bands which are assigned to different cells (In cellular communications, a cell refers to the hexagonal/circular area around the base station antenna). However, after certain geographical distance, the frequency bands are re-used, i.e. the same spectrum bands are reassigned to other distant cells. The co-channel interference arises in the cellular mobile networks owing to this phenomenon of Frequency reuse. Thus, besides the intended signal from within the cell, signals at the same frequencies (co-channel signals) arrive at the receiver from the undesired transmitters located (far away) in some other cells and lead to deterioration in receiver performance.

Adverse weather conditions: During periods of uniquely high-pressure weather, VHF signals which would normally exit through the atmosphere can instead be reflected by the troposphere. This tropospheric ducting will cause the signal to travel much further than intended; often causing interference to local transmitters in the areas affected by the increased range of the distant transmitter.

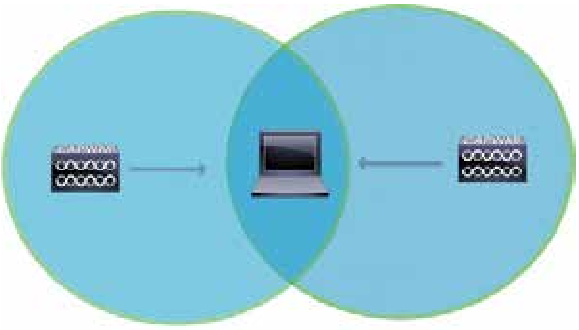
Poor frequency planning: Poor planning of frequencies by broadcasters can cause CCI, although this is rare. A very localised example is Listowel in the south-west of Ireland. The 2RN UHF television transmitter systems in Listowel and Knockmoyle (near Tralee) are on the same frequencies but with opposite polarisation. However, in some outskirts of Listowel town, both transmitters can be picked up causing heavy CCI. This problem forces residents in these areas to use alternative transmitters to receive RTÉ programming. Another example is the surrounding area of viewers that can receive mainly Gunung Ledang transmitter in Malaysia. Examples are TV1 and TV2 from Bukit Tinggi and Bukit Tampin, who are using both Channel 6 and Channel 9. Moreover, Negeri FM from Bukit Tampin and Asyik FM from

Gunung Ledang, which frequencies are 95.7 MHz and 95.6 MHz respectively. TV3 and TV1 from Gunung Ledang and Suria and Channel U from Singapore also using same frequency, who are using both Channel 12 and Channel 28. That Channel 12 and 28 from Ledang transmits in high TX power, causing interference in most of Johor area, but viewers are still able to receive TV station from Gunung Pulai (Johor Bahru) well. This causing difficulty for viewers who watching using analogue TV, and needs to using alternate transmitter or even using better antenna for better reception, or force them to subscribe Astro/buying NJOI satellite or Unifi Fibre service/use DVB-T2 set top box for Singapore DTT reception. In addition, Minnal FM from Gunung Kledang, Ipoh which transmits to Central Perak and 988FM from Gunung Ulu Kali which transmits to Klang Valley and South Perak, which are on 98.9 MHz and 98.8 MHz respectively. The 98.9 MHz can transmits to most of Perak area, causing interference in most of Perak area, but listeners are still able to tune to Minnal FM on 96.3 MHz from Gunung Ulu Kali (Klang Valley, South Perak and Tapah) or 107.9 MHz from Maxwell Hill, Taiping, and 988 on 99.8 MHz from Gunung Kledang, Ipoh. Another case is an Islamic channel TV Alhijrah, which three of the transmitters, Gunung Ulu Kali, Gunung Keldang and Bukit Tampin, all using the same frequency of 743.25 MHz, will causing interference in some areas and therefore some areas cannot even receiving the channel. Affected areas must use Astro,NJOI or Unifi IPTV to receive this channel.

Overly-crowded radio spectrum: In many populated areas, there just isn't much room in the radio spectrum. Stations will be jam-packed in, sometimes to the point that one can hear loud and clear two, three, or more stations on the same frequency, at once. In the USA, the FCC propagation models used to space stations on the same frequency are not always accurate in prediction of signals and interference. An example of this situation is in some parts of Fayetteville, Arkansas the local 99.5 FM KAKS is displaced by KXBL 99.5 FM in Tulsa, particularly on the west side of significant hills. Another example would be of Cleveland's WKKY 104.7 having interference from Toledo's WIOT 104.7 FM on the Ontario shore of Lake Erie, as well as Woodstock's CIHR-FM (on rare occasions), which is also on 104.7 FM, due to the signals travelling very far across Lake Erie. The interference to WIOT from the operation of W284BQ, translator, has been resolved by the FCC. Effective October 18, 2011 it must cease operation.

Daytime vs Nighttime: In the Medium frequency portion of the radio spectrum where most AM broadcasting is allocated, signals propagate full-time via groundwave and, at nighttime, via skywave as well. This means that during the nighttime hours, co-channel interference exists on many AM radio frequencies due to the medium waves reflecting off the ionosphere and being bounced back down to earth. In the United States, Canada, Mexico, and the Bahamas, there are international agreements on certain frequencies which allocate "clear-channel" broadcasting for certain stations to either have their respective frequencies to themselves at night, or to share their respective frequencies with other stations located over hundreds or even thousands of miles away. On other frequencies, there are "Regional Channels" where most stations on these frequencies either reduce power or change to a directional antenna system at nighttime to help reduce co-channel interference to each other's signals. In the United States, there are six "Local Channel" frequencies, also known as "graveyarders" where nearly every station on those frequencies has the same power and antenna pattern both day and night and, as a result of skywave propagation, there is normally massive co-channel interference in rural areas on these frequencies, often making it difficult, if not impossible, to understand what's being said on the nearest local station on the respective channel, or the other distant stations which are bouncing on the same channel, during the nighttime hours. Skywave has been used for long distance AM radio reception since radio's inception and should not be construed as a negative aspect of AM radio. FCC deregulation allowed many new AM radio stations on the former clear and regional channel designations; this is the principal cause of overcrowding on the AM band at night. A new source of interference on the AM broadcast band is the new digital broadcast system called HD, any AM station that broadcasts HD superimposes digital "hash" on its adjacent channels. This is especially apparent at night as some stations, for example WBZ transmits its 30 kHz wide signal for hundreds of miles at night causing documented interference and covering another station on an adjoining frequency (WYSL 1040) as far as 400 miles away.

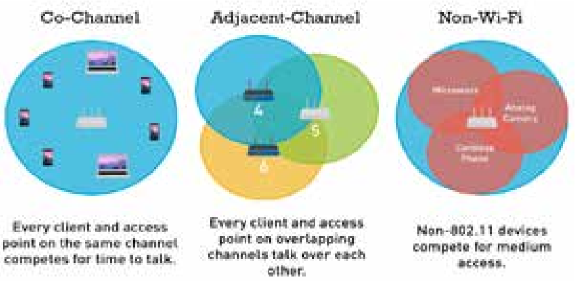
Cancellation of signal: In addition, many AM stations, including but not limited to the clear channel stations, often experience cancellation of their own signals within the inner and outer fringes of their normal groundwave coverage areas at nighttime due to the stations' individual skywave signals reaching the listeners' receivers at or near equal strength to the stations' individual groundwave signals; this phenomenon is very similar to the multipath interference experienced on FM Radio in the VHF band within mountainous regions and urban areas due to signals bouncing off of mountains, buildings, and other structures, except that the groundwave-skywave cancellation occurs almost exclusively at nighttime when skywave propagation is present.



Basic CCI – AP's on the same Channel interfere with one another

3. Adjacent Channel Interference

Adjacent Channel Interference is interference caused by extraneous power from a signal in an adjacent channel. ACI may be caused by inadequate filtering (such as incomplete filtering of unwanted modulation products in FM systems), improper tuning or poor frequency control (in the reference channel, the interfering channel or both). ACI is distinguished from crosstalk



Every client and access point on the same channel competes for time to talk.

Every client and access point on overlapping channels talk over each other.

Non-802.11 devices compete for medium access.

Co-Channel interference isn't a major problem until there are too many WiFi devices on the same channel. Adjacent-Channel interference on the other hand is where you run into problems and channel selection becomes critical. Luckily, these channel related interferences can be reduced or eliminated by selecting the proper WiFi channel for your network.Using a spectrum analyzer like inSSIDer Office will allow you to see this wireless environment, so you can either select the right channel or mitigate WiFi interference. Ulti-

mately, improving your 2.4 GHz WiFi network performance.

Non-Overlapping Channels

Each channel on the 2.4 GHz spectrum is 20 MHz wide. The channel centers are separated by 5 MHz, and the entire spectrum is only 100 MHz wide total. This means that the 11 channels have to squeeze into the 100 MHz available, and in the end, overlap.

Effects of interference

- A decrease in the wireless range between devices
- A decrease in data throughput over Wi-Fi
- Intermittent or complete loss of the wireless connection
- Difficulty pairing during a Bluetooth device's discovery phase

Sources of interference

- Microwave ovens: Using your microwave oven near your computer, Bluetooth device, or Wi-Fi base station may cause interference.
- Direct Satellite Service (DSS): The coax cable and connectors used with certain types of satellite dishes may cause interference. Check the cable for damage and obtain newer cables if you suspect RF leakage issues.
- Certain external electrical sources such as power lines, electrical railroad tracks, and power stations.
- 2.4 GHz or 5 GHz phones: A cordless telephone that operates in this range may cause interference with wireless devices or networks when used.
- Video senders (transmitters/receivers) that operate in the 2.4 GHz or 5 GHz bandwidth.
- Wireless speakers that operate in the 2.4 GHz or 5 GHz band.
- Certain external monitors and LCD displays: Certain displays may emit harmonic interference, especially in the 2.4GHz band between channels 11 and 14. This interference may be at its worst if you have a portable computer with the lid closed and an external monitor connected to it. Try changing your access point to use 5 Ghz or a lower 2.4 GHz channel.
- Any other wireless devices that operate in the 2.4 GHz or 5 GHz bandwidth (microwaves, cameras, baby monitors, neighbors' wireless devices, and so on).

Some beliefs of Wifi Interferencesconclusions

1. "There are just a few easy-to-find devices that can interfere with my Wi-Fi."

With the huge proliferation of wireless devices in the unlicensed band, it is no longer obvious what might be a source of interference-wireless links are now embedded in watches, shoes, MP3 players, and many other tiny consumer devices.

In some cases, previously benign devices have been updated with RF technology. Motion detectors, which appear in many offices for lighting control, are a good example. A new breed of hybrid motion detectors uses a combination of passive infrared sensor (PIR) and 2.4-GHz radar to detect motion. These devices, which look identical to their benign predecessors, generate significant interference that can disrupt your Wi-Fi network.

Unintentional emitters are also hard to find. A defective ballast on a fluorescent light fixture can generate broadband RF interference that can impact Wi-Fi. This is impossible to identify by simply looking at the device. "Hidden devices" are becoming more common as well. We have seen numerous instances where a security group has hidden wireless cameras-unbeknownst to the networking group-not realizing that they are jamming the Wi-Fi network.

2. "When interference occurs, the impact on data is typically minor."

The impact of a single interferer on data throughput (or data capacity) of your Wi-Fi network can be astounding.

There are three major factors that determine the impact of an interference device:

• **Output power.** The greater the output power, the larger the physical "zone of interference" the device creates.

• **Signal behavior with respect to time.** Analog devices, such as some video cameras and older cordless phones, have a constant always-on signal. Digital devices, such as digital cordless phones, tend to "burst" on and off. Different devices have varying durations of on-time and off-time. In general, the greater the percentage of time that the signal is "on" and the more frequently it bursts, the greater the impact it will have on throughput.

• **Signal behavior with respect to frequency.** Some devices operate on a single frequency, and impact specific Wi-Fi channels. Other devices hop from frequency to frequency and impact every channel but to a lesser degree. Some devices, such as microwave ovens and jammers, sweep quickly across the frequency spectrum, causing brief but serious interruptions on many frequencies.

A recent study undertaken by Farpoint Research measured the impact of various interference devices on the data throughput of Wi-Fi. At 25 feet from the AP or client, a microwave oven was found to degrade data throughput by 64 percent, a frequency-hopping phone degraded throughput by 19 percent, and an analog phone and video camera both degraded throughput by 100 percent (in other words, no ability to connect).

Summary: Interference can really take the zip out of your Wi-Fi data throughput.

3. "Voice data rates are low, so the impact of interference on voice over Wi-Fi should be minimal."

With modern voice coding, the data rate of an individual voice call is on the order of 8 Kbps. Compared to the maximum throughput of a Wi-Fi network, this seems like a trivial amount, and it therefore seems reasonable to expect that a Wi-Fi access point can handle many concurrent voice-over-IP (VoIP) calls.

Unfortunately, many factors reduce the number of calls that an access point can handle. First, there is significant VoIP protocol-level overhead, which increases the typical stream to 100 Kbps. Then there is additional protocol overhead imposed by Wi-Fi. Second, voice traffic is very sensitive to jitter and delay, requiring extra capacity in the network to minimize congestion. The typical number of voice calls that vendors advertise they can handle with a Wi-Fi access point is only 15. When interference is introduced, the number of calls that can be handled drops from there.

In addition, small amounts of interference seriously impact voice-over-Wi-Fi voice quality. A recent study undertaken by Farpoint Research measured the impact of various interference devices on the mean opinion score (MOS) for voice-over-Wi-Fi calls, and found the voice quality falling to unacceptable levels when a microwave, cordless phone, video camera, or co-channel Wi-Fi device was within 25 feet of the access point or phone. And perhaps more importantly, interference creates coverage holes where phone calls will be dropped. An in-house study showed that the effective range of a VoWi-Fi phone drops by 50 percent with an interference device (cordless phone or video camera) at a distance of 75 feet from the access point. This 50 percent reduction in the range of your phones would likely result in coverage holes over 75 percent of your floor space.

4. "Interference is a performance problem, but not a security risk."

If an Internet worm got through your corporate firewall and was using up 50 percent of your corporate network bandwidth as it spread from machine to machine, would you consider that a security or a performance concern? The point here is that anything that impacts mission-critical corporate IT systems is a security concern. As your corporate Wi-Fi network becomes more and more mission-critical, any possible interference device-whether the interference is malicious, as in the case of a jammer, or accidental-must be viewed as a potential security issue. In addition to RF denial of service, there are several other risks related to non-Wi-Fi RF devices, including:

- **Multiprotocol devices.** Wi-Fi networks are typically locked down with secure access controls, but devices that run on non-Wi-Fi networks, such as Bluetooth devices, are not. A notebook computer with Wi-Fi and Bluetooth connectivity may act as bridge, allowing an intruding device onto the corporate LAN or WLAN. Preventing accidental bridging between insecure networks and the corporate networks requires: 1) client-based tools that control configuration of wireless network interfaces, and 2) RF monitoring that watches for suspicious non-Wi-Fi activity indicating possible bridging.

- **Non-Wi-Fi rogues.** Most enterprises implement some form of Wi-Fi rogue access point detection to find unauthorized (and frequently unsecured) access points on the corporate network. But there are non-Wi-Fi devices (such as Bluetooth access points) that can open up a similar security hole. Like Wi-Fi rogues, these devices must be detected and eliminated.

- **Leakage of sensitive data.** Certain non-Wi-Fi devices such as cameras and cordless phones can be used to carry sensitive data out of a restricted area, bypassing corporate security policies. When this is a concern, a zone of restricted wireless operation should be established, and that zone should be enforced through monitoring of the spectrum for unauthorized devices.

5. "802.11n and antenna systems will work around any interference issues."

Systems that use multiple antennas or smart antennas are able to increase immunity to interference by boosting the desired signal seen at a receiver. When the desired signal is stronger, the ratio of that signal to interference (referred to as signal-to-noise ratio or SNR) is also improved. Effectively, this reduces the zone of interference associated with a particular interference device to a smaller area. But the gain achieved by a smart antenna system is typically only on the order of 10 dB of enhanced signal power. This means that the range of interference might be shrunk by a factor of 2 over a traditional antenna system, but even then the interference problem is far from solved. For example, if a device would have previously caused problems at a distance of 80 feet from the receiver, it will still cause problems up to 40 feet from the receiver. Thus you would have 5000 square feet of floor space where the interference is still a problem.

CONCLUSION

In this paper, we consider about the interferences of wifi network 802.11 and discussed about the co channel interference and adjacent channel interference in the wifi networks and finally we have given some myths of wifi deployment. Even though we have many avoidance methods both for co-channel interference and adjacent channel interference this paper helps to understand the interferences in wifi and to work on finding a solution for above interferences.

REFERENCE

[1]http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert wifi/prod_white_paper0900aecd807395a9.htmlriate. [2] https://en.wikipedia.org/wiki/Co-channel_interference [3]http://www.metageek.com/training/resources/why-channels-1-6-11.html [4]https://support.apple.com/en-us/HT201542.