Analysis of the impact of electromagnetic interference on the performance of a household wireless network

Jasmin Muratović*, Karlo Josić * and Silvio Papić*
* Algebra University College, Zagreb, Croatia
Silvio.papic@algebra.hr

***Abstract* - Today, more than 90% of households in the EU have internet access and use wireless network technologies to a large extent. With the increasing penetration of the Internet of Things (IoT), access to the Local area wireless network is under increasing load. In this paper, an analysis of the living space of a typical multi-member family in an urban environment in Croatia and the impact of different sources of electromagnetic radiation on the performance of a local wireless network is made. Primarily 2.4 GHz frequency spectrum was analyzed, and the influence of different individual sources of electromagnetic radiation on the quality of communication via a local wireless network was determined using different communication analysis tools. The contribution of this paper is to bring into focus common, invisible to us humans, communication problems due to the overcrowded 2.4 GHz space of a typical urban household, which can certainly affect the performance of the Internet of Things environment in new more modern homes. As a result of this research are recommendations and guidelines on how to distribute and use sources of electromagnetic radiation in the household to avoid major interference to the wireless network communication signal.**

Keywords - Wireless Networks; Wi-Fi; Wi-Fi Spectrum analysis; IoT

I. INTRODUCTION

In wireless network environments, data transmission takes place via high-frequency radio waves. Wi-Fi is the most popular wireless technology that carries internet protocol (IP) traffic [1]. In most of today's households, wireless networks are used for laptops and smartphones to access the Internet. Wi-Fi brings people, processes, data, and devices, together and enables using data and transform it into valuable information that makes life better and business thrive [2]. Requirements for higher data transmission speeds of wireless communication are increasing daily which is necessary to accommodate for all the new devices with more and more data throughput hungry applications. To connect these devices to a wireless network, two frequency spectrum are used today 2.4GHz and 5GHz. Besides security concerns regarding this shared data transmission media, a big challenge is all the interference for the signal itself. Because wireless networks are used for the transmission of data via microwaves on certain radio frequencies, which represent the physical layer of the network, they are sensitive to various sources of interference. The more devices are trying to use the same wireless network they will be in contention for the access and usage of the wireless network itself which is normal because of the nature of the wireless network. Also, there are issues regarding the environment in which the wireless network operates that are also influencing how the signal is propagated, what is the signal strength in certain areas of the network, etc. These two issues are part of the wireless network itself and the way we design and deploy the wireless network. But there is a third aspect and this is something that normally is introduced to the wireless environment without prior consideration about how it will impact the wireless signal, especially in the home environments. These are different sources of electromagnetic signals that interfere with existing wireless network signals. These are not just other wireless access points from your neighbor but also various devices that we use in our homes daily like Bluetooth devices for a gaming console, headphones, baby monitors, smartwatches, microwave ovens, etc. In this paper, we analyze how various sources of wireless signal present in today's homes are influencing wireless network performance. Primarily we focused on the 2.4 GHz frequency spectrum because of the saturation that is becoming more obvious every day and now regular users are starting to notice the diminished performance of their wireless network which is usually interpreted as „slow Internet“. After the analysis is done we can make some general conclusions about how these new wireless devices are affecting wireless network performance.

II. WIRELESS LAN AND FREQUENCY RANGE

In this section, a short overview of current wireless local area network technologies will be given. There are different kinds of wireless networks depending on their function and coverage area. When we talk about a network in an average household this network is called Local Area Network (LAN) and if this is a wireless network that it is called Wireless Local Area Network (WLAN). Acronym WLAN implies an IEEE 802.11 set of standards that are used for the development of wireless technologies on layer 1 and layer 2 of the Open Systems Interconnection (OSI) model. In everyday speech, we refer to wireless local area networks as Wi-Fi networks which is a brand term coined by the brand-consulting firm *Interbrand* just so that it would be easier to remember than the original name *IEEE 802.11b direct sequence*. A network of companies that drives global adoption of wireless technologies based on the IEEE 802.11 set of standards is called the Wi-Fi alliance. (Wi-Fi Alliance, 2021) Some of the most used standards today are 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac. Devices that operate by these 802.11 standards are using two frequency spectrum one in a 2.4GHz range divided into 11 or 13 channels separated by 22 MHz as shown in Figure 1, and one in a 5GHz range (which is 5.17GHz - 5.33GHz) which is very flexible in terms of channel width using channel binding techniques.

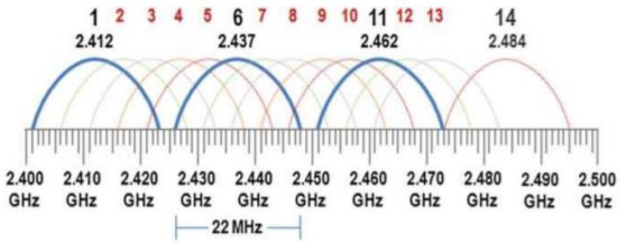

Figure 1. WLAN channels in 2.4 GHz band [3]

All of today's wireless devices support one of these spectrums or even both. There are some advantages and drawbacks of each frequency range that needs to be taken into account when designing wireless networks. Most of the time typical wireless network will use both frequency ranges because of various wireless devices that connect to a wireless network. For example, because the frequency level 2.4GHZ range has a better range for the same signal strength than 5GHz but because of the congestion of the 2.4GHz range, it is more prone to interference from other sources. Also, still, not all devices support 5GHz although much higher data rates are possible. Figure 2 shows the overview of standards and their characteristics.

Standard	Freq Band	Bandwidth	Modulation	Max Data Rate
802.11	2.4 GHz	20 MHz	DSSS,FHSS	2 Mbs
802.11b	2.4 GHz	20 MHz	DSSS	11 Mbs
802.11a	5.0 GHz	20 MHz	OFDM	55 Mbs
802.11g	2.4 GHz	20 MHz	DSSS,OFDM	55 Mbs
802.11n	2.4 GHz, 5.0 GHz	20 MHz,40 MHz	OFDM	600 Mbs
802.11ac	5.0 GHz	20 MHz,40 MHz, 80 MHz,160 MHz	OFDM	6.93 Gbs

Figure 2. IEEE 802.11 standards overview

III METHODOLOGY

For this paper analysis of wireless interference will be conducted in an apartment in the municipal building in Zagreb. The apartment has an area of around 100 m2 and is located on the 8th floor. Building construction s of steel-reinforced concrete bearing walls and drywall partition wall. The ground plan of the apartment is shown in figure 3.

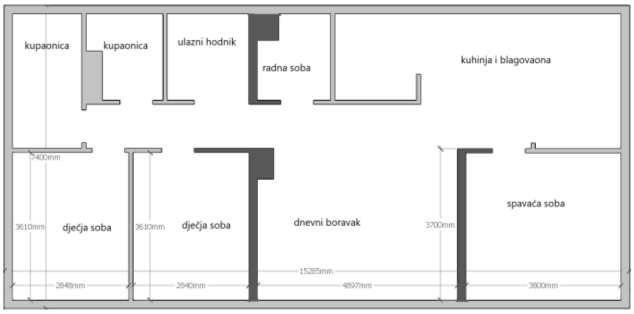

Figure 3. The ground floor of the apartment

There is one wireless access point in the apartment centrally located. The signal strength of the wireless access point is set to maximum so that every part of the apartment is covered and that the wireless access point is utilized to the maximum. The frequency spectrum that will be analyzed is 2.4GHz. For the interference sources, we will test Bluetooth devices, microwave ovens, gaming console gadgets, cordless phones, wireless cameras, baby monitors, remote control devices, Virtual reality goggles, and wireless access points. For testing, we used Cisco WAP4410N wireless access point, USB wireless LAN network interface card model DWA-127 for network scanning purposes, and the USB RF Explorer interference measuring device. Measurements of interference between Wi-Fi and IoT devices were made at a distance of 1 m from each other. Access point broadcasts a signal with a power of 100mW on a channel bandwidth of 20 Mhz. We connected two Wi-Fi devices to the wireless access point and started communication between them by sending larger files. In such an environment, we measured and compared two key data: latency and percentage of retransmitted packets. These two data are key indicators of the impact of individual IoT devices on Wi-Fi network performance. In the continuation of the paper, we present an analysis and impact measurement of an individual IoT device on the performance of the Wi-Fi network with a tabular display and a comparison of all devices included by this work.

III. MEASUREMENTS

Before taking any measurements a heatmap was created to see if the usable signal from the main access point is covering the entire area of the apartment. This is important just to confirm that taking measurements makes sense because comparison will be done by measuring signal strength directly. The heat map is shown in figure 4.

Figure 4. Heatmap of the wireless signal

The heatmap reveals the position of the main wireless access point and the measurement was done along the line every at points 1 meter apart. From this Heatmap it is evident that signal strength is getting weaker as the signal is passing through the walls, especially through steel-reinforced concrete bearing walls. Nevertheless, the signal strength is still adequate in all parts of the apartment to support wireless communication. Although signal strength is adequate this is not enough to conclude that this wireless network will function in all circumstances. To see how other devices that emit electromagnetic radiation influence the Wi-Fi signal we will also need to create a baseline for this wireless network to compare future readings. This baseline measurement is done 1 m from the main access point when all other devices are turned off. The result of this measurement was that the interference signal is -80 dBm which is below levels that could influence the main access point wireless signal. Using the Wireshark tool it is established that the average packet loss was 8.4%. This high data retransmission is due to neighboring wireless access points in other apartments that are using overlapping channels. The first measurement of interfering wireless signal was done using Bluetooth headphones version 1.1. Setup was that Bluetooth headphones are receiving music while a file was copied between two laptops connected over a Wi-Fi network. Inter is in the frequency range from 2460 – 2480 MHz which is directly overlapping with the Wi-Fi signal. In normal operation, if a Bluetooth device transmits on a frequency that overlaps with the Wi-Fi channel while a Wi-Fi device is in the "listen before transmit" phase, the Wi-Fi device will do a random backoff during which time the Bluetooth device will hop to a non-overlapping channel allowing the Wi-Fi device to begin its transmission [4] which causes delays. The result on the wireless network was functionally the same as a Denial Of Service (DoS) attack. Data loss was 32,8% and latency was up to 3016ms which is a practically unusable network for most of the applications. A microwave oven has a similar influence on the wireless network. The microwave oven does not transmit data, but still radiates signals in the unlicensed 2.4 GHz band acting as an unintentional interferer for IEEE 802.11 Wireless Fidelity (Wi-Fi) communication signals [4]. Although microwave ovens should shield from microwave radiation this is not the case. Also, although the declaration of the microwave oven (Samsung M1717N) states that the frequency is 2450 GHz the interference is through the most of Wi-Fi 2.4 GHz range and the interference signal strength is very high at 3 meters from the oven and still sensible even at a 5-meter distance from the oven. Fortunately, there is a technique for mitigating microwave oven interference called a cognitive radio system. It is possible to transmit data without any microwave oven interference during the OFF cycles of the microwave [5]. This was expected from the microwave oven but even worse are wireless cameras that are becoming common devices in modern homes. For the measurement, we used a typical wireless camera that is easy to install which makes it a popular choice (model 203CWAS). Just from the signal measurement, it was clear that this is a very strong and stable interference measuring -40dBm at a 3 m distance from the main Access point. When we tried to use a wireless network just for basic file transfer between two laptops the network just failed after less than 30 seconds of very poor performance. To our surprise Wi-Fi camera was the worst device that you can have in your wireless network. All of these measurements were done one by one without simultaneous usage of different interference sources. We also took measurements of interference signal strength from other sources namely Cordless phones which do not affect the Wi-Fi network because of the different frequency range (1900MHz). Video Baby monitor (model Miao-Miao) does not influence the Wi-fi network because of a very weak signal that reaches only 5-6 meters. Other Bluetooth devices like gaming consoles (Sony Play Station 4) and remote control toy cars had a negligible effect on the Wi-Fi network performance. One interesting thing to note is how the Wi-Fi network adapts to user devices that use different 802.11 standards namely 802.11 b. In the case when you have at least one 802.11b device the performance of the Wi-Fi network will diminish for all of the devices although other devices are using standards that support higher speeds. In our case retransmission rate when only one 802.11b devices was connected was 29% with latency as high as 1627ms. The results can be seen in table 1.

Table 1 Measurement results

Device	***Max. Latency (ms)***	***Max (dBm)***	***Network Data rate (Mb/s)***	***Data loss (%)***
Bluetooth earphones standard 1.1	3061	-42	1	32.8
Microwave oven at 3 m	3016	-32	3.5	19.7
Game console	130	-54	3.5	9
Cordless phone	No effect	N/A	No effect	0
Wireless camera	>10000	-42	1	100
802.11 b device	1627	-62	3.5	29

IV. Conclusion

Measuring these electromagnetic interferences we saw that all sorts of devices can interfere with Wi-Fi signal even if the declaration says they should not interfere. The fact of the matter is that the average Wi-Fi user will not create Heatmaps and do a site survey to analyze the wireless environment for interferences or overlapping channels between wireless access points. Because more and more wireless-capable devices, especially IoT devices are becoming normal in modern homes at least some guidelines should be followed when choosing and using these devices. Recommendation based on the data collected and analyzed is to choose devices that support the 5 GHz range, change old devices with newer ones that are less prone to interfere with the Wi-Fi network. Use wireless access points that can automatically adjust operating frequency and adjust signal strength to overcome interference. Do not use multiple devices that emit electromagnetic signals (microwave ovens and wireless cameras). Soon even the 5GHz range will suffer from similar problems as the 2.4GHz range but this is inevitable because of the nature of wireless technology which is a shared media that all wireless devices can access or just interfere with.

References

[1] K. Pahlavan and P. Krishnamurthy, “Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective,” *Int. J. Wirel. Inf. Networks*, vol. 28, no. 1, pp. 3–19, 2020, DOI: 10.1007/s10776-020-00501-8.

[2] K. K. K. Fong and S. K. S. Wong, Wi-Fi Adoption and Security in Hong Kong, Asian Social Science, Vol. 12, No. 6, pp. 1–22, 2016.

[3] S. Lepaja, A. Maraj, and S. Berzati, “WLAN Planning and Performance Evaluation for Commercial Applications,” *Lect. Notes Data Eng. Commun. Technol.*, vol. 20, no. November, pp. 53–69, 2019, DOI: 10.1007/978-3-319-94117-2_3.

[4] A. Mahajan and S. Gupta, “Interference Evaluation of Different Wireless Systems Operating in 2 . 4 GHz ISM Band,” *NCVSComs-13*, pp. 3–6, 2012.

[5] Tanim M. Taher, Matthew J. Misurac, Joseph L. LoCicero, Donald R. Ucci, “Microwave oven signal interference and mitigation for Wi-Fi Communication systems,” Department of Electrical and Computer Engineering, Illinois Institute of Technology Chicago, IL 60616