HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 3. szám 133–152.
DOI: 10.32567/hm.2022.3.9

Zsolt Haig,[1] Zsolt Illési,[2] János Péter Varga[3]

Possibilities of Electronic Jamming of WLAN Networks in the Physical Layer

Wireless local area networks or WLANs are the necessary underlying communication technology of consumer electronics, mobile computers and mobile phones of our days. Thanks to the comfortable operations and ubiquitous applicability for work and entertainment, the demand surged for these devices in the last 15 years. WLAN solutions provide the opportunity for mobility. But these networks communicate via radio waves with devices, which can be eavesdropped on and attacked. One form of attack is jamming. This article analyses the most frequent WLAN standards and the jamming options, particularly the execution of electronic jamming in the physical layer.

Keywords: WLAN, wireless networks, jamming, SDR

1. Introduction

These days civilian society is also greatly dependent on wireless communication. Therefore, the confidentiality, integrity and availability of radiofrequency communication are a growing concern due to the widespread security threats. Wireless networks, and thus WLAN, are susceptible to software attacks, which are widely used against computer networks and vulnerable to eavesdropping and especially radio jamming. Attackers can exploit the access to the radio frequency communication channel without physical connection, making jamming more beneficial.

In the context of this scientific problem, the aim of this paper is to systematise the attacks, namely electronic jamming that can be applied at the physical layer against WLANs. A further goal is to experimentally prove that jamming is an effective form of attack against WLAN. To achieve these goals, we first provide a literature overview and then perform a measurement of some WLAN jamming methods in a test environment.

[1] Professor, University of Public Service, e-mail: haig.zsolt@uni-nke.hu
[2] Associate Professor, Milton Friedman University, e-mail: illesi.zsolt@uni-milton.hu
[3] Associate Professor, Óbuda University, e-mail: varga.peter@kvk.uni-obuda.hu

2. WLAN technology

Wireless local area network (WLAN) solutions are based on the IEEE 802.11 standard. Laptops, tablets, smartphones and consumer electronics devices use this technology for communications. There are two frequency bands within the radio spectrum the WLAN devices can communicate in a local area network. These frequency bands were divided into channels to permit identification. Selecting a channel within a frequency band plays an important role. It is inevitable to plan the allocation of these channels to maximise the overall performance of wireless networks where multiple access points are used at close quarters, like in an office building or a housing estate. The local networking solution of the technology addresses the unauthorised use of the spectrum. This was solved in two frequency bands. The first is the Industrial, Scientific and Medical (ISM) band in the 2.4 GHz range. The second is the Unlicensed National Information Infrastructure (UNII) band in the 5 GHz range. Devices can be operated in these frequency bands without special licences under specific conditions. ISM and UNII bands can be used not only by WLAN devices. Thus, for example, particular devices might be jamming each other. The IEEE 802.11 standard family defines multiple transfer modes and protocols, of which the 802.11n (Wi-Fi 4), the 802.11ac (Wi-Fi 5) and the 802.11ax (Wi-Fi 6) are the most widely used ones. The following table shows the parameters of the standard family.[4]

Table 1: Key parameters of 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5) and 802.11ax (Wi-Fi 6)

PARAMETER	**IEEE 802.11N (Wi-Fi 4)**	**IEEE 802.11AC (Wi-Fi 5)**	**IEEE 802.11AX (Wi-Fi 6)**
Maximum data rate (Mbps)	600	6930	9607
RF Band (GHz)	2.4 or 5	5	2.4 or 5
Modulation type to maximum data rate	64-QAM	256-QAM	1024-QAM
Channel width (MHz)	20 or 40	20, 40, 80 or 160	20, 40, 80 or 160

Source: Wi-Fi Channels, Frequencies, Bands & Bandwidths. Electornics Notes, s. a.

Developers created a variety of methods in the Wi-Fi 4, 5, 6 standards, ensuring that wireless networking solutions can serve user demands and eliminate the opportunity that the wireless network could be the bottleneck in the system.

The experiments described in this paper are testing the potential options of the electronic jamming of n and x devices of the 802.11 standard families in the 2.4 GHz frequency band. After that, the paper summarises the related parameters of these WLAN ranges.

Both 802.11n ac and ax standards apply quadrature amplitude modulation (QAM) to maximise data transfer. The advantages of the modulation are the effective

[4] Rashmi Bhardwaj: Wi-Fi generation comparison Wifi6 vs Wifi5 vs Wifi4. *Network Interview,* s. a.

utilisation of the bandwidth. This method ensures the effectiveness of the data transmission of the radio communication. A significant disadvantage of this modulation method is the noise sensitivity. The transmission states are too close to each other. This issue is illustrated in Figure 1.

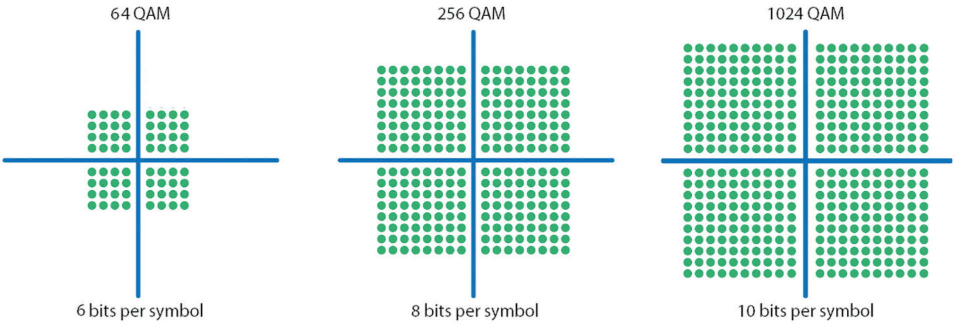


Figure 1: 64-QAM, 256-QAM and 1024-QAM states

Source: QAM modulator and demodulator. Faststream Technologies, 28 February 2022.

WLAN technology ensures that multiple users can use the available resources simultaneously. The Orthogonal Frequency-Division Multiplexing (OFMD) and Orthogonal Frequency-Division Multiple Access (OFMDA) permit it. The OFDM supports Time Division Multiple Access (TDMA) connections, while OFDMA or Frequency Division Multiple Access (FDMA) provide user support. The following figure illustrates the difference between OFDM and OFDMA.[5]

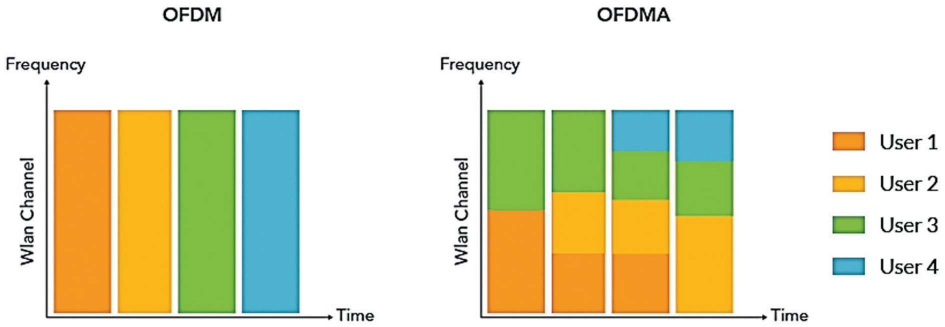


Figure 2: OFDM and OFDMA modulation

Source: Eve Danel: Wi-Fi 6's OFDMA Challenges Make Verification Crucial. RF Globalnet, 02 December 2019.

[5] Caleb McKee: *OFDMA vs OFDM explained.* 04 March 2021.

802.11n and 802.11ac standards support OFDM, while 802.11ax now supports OFDMA technology.

2.1. WLAN 2.4 GHz channels

WLAN devices in the 2.4 band provide 13 distinct channels in Europe, distributed by 5MHz from each other. Three non-overlapping channels are available when considering 20 MHz bandwidth channels. The following figure illustrates this.

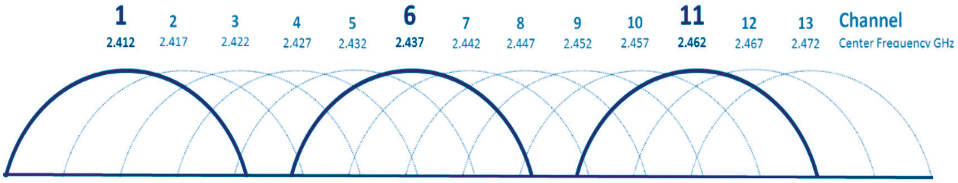


Figure 3: 64- Non-overlapping channels in the 2.4 GHz WLAN band
Source: Wi-Fi 4/5/6/6E (802.11 n/ac/ax). Duckware, 03 September 2022.

It is possible to find 20–30 WLAN Access Points (AP) in the overall 13 channels in some geographical areas due to the spread and the rapid development of the 2.4 GHz band-related technologies. These devices share those 13 channels, meaning that some of these operate overlapping and interfere with each other. There is a possibility of using 802.11n devices for channel bonding, making 40MHz bandwidth channels possible. Of these 40 MHz channels, only two are non-overlapping. Therefore, these bonded channels are prone to higher noise emitted by the other channels. Applying bonded channels requires a compromise between the throughput of the channel and signal quality.

2.2. Received Signal Strength Indicator and Signal/Noise Ratio

The Received Signal Strength Indicator (RSSI) is a value measured by the user device, which specifies signal quality. The measurable value is a relative number. The higher the number, the better the signal quality. The scale is from –100 to 0. The RSSI unit is dBm. The following table illustrates signal quality levels related to these values.[6]

[6] What is WiFi Strength and RSSI? *SimpliSafe,* s. a.

Table 2: RSSI value and Signal Strength

RSSI Value	Signal Strength
> -40 dBm	Perfect
-50 to -40 dBm	Excellent
-60 to -50 dBm	Very good
-70 to -60 dBm	Good
-80 to -70 dBm	Fair
-90 to -80 dBm	Poor
< -90 dBm	No connection

Source: Compiled by the authors based on What is WiFi Strength and RSSI? SimpliSafe, s. a.

The ability of the receiver device to separate the background signals of a given radio spectrum from its own plays a crucial role in wireless communication solutions. The Signal/Noise Ratio (SNR) indicator was introduced to measure this.

The SNR value indicates the relationship between the signal to noise. The SNR unit is dB. The unwanted or undesirable information for the receiver is the noise. The noise could stem from radio traffic of other units or malfunctioning devices. The SNR value shows whether the quality of the selected communication channel is adequate. The following table indicates the quality classifications for SNR values.[7]

Table 3: SNR value, Signal quality and WLAN signal indication

SNR Value	Signal quality	WLAN signal indication
> 40 dB	Excellent	▂▄▆█
25 to 40 dB	Very good	▂▄▆
15 to 25 dB	Low	▂▄
10 to 15 dB	Very low	▂
5 to 10 dB	No signal	

Source: Compiled by the authors, based on Signal-to-Noise Ratio (SNR) and Wireless Signal Strength. CISCO, s. a.

These classifications visualise the quality of the AP and the channel between the user. This feedback also shows the user which services can be used fault-free. Above 40 dB all services of the communication channels shall be used. Between 5 and 10 dB, the noise level is so high that it is impossible to differentiate it from the sender's signal. Electronic jamming is to be used if the aim is to deny communication.

[7] Signal-to-Noise Ratio (SNR) and Wireless Signal Strength. *CISCO*, s. a.

3. Basics of electronic jamming

Electronic jamming is an electronic attack method that came out with radios in the military at the beginning of the 1900s. Electronic jamming is, in military terms, the subset of electronic warfare. Electronic warfare aims to gather intelligence and deny the operations of systems operating in the electromagnetic spectrum of the adversary and maintain the operational capabilities of its similar systems. Jamming in military operations is a widely used action. The aim is to curtail the operations of the receiver units of the electronic devices used by the adversary's intelligence, command and control systems and deny the reception of signals carrying information.[8]

Figure 4 illustrates the general geometry of the jamming of radio communication networks and the main factors to consider. An essential precondition of effective jamming is to identify the characteristics (e.g. frequency, power, modulation) of the network to be jammed. These pieces of information can be collected by Communication Intelligence (COMINT). Jamming always appears at the receiver. Therefore, it is necessary to analyse the signal-to-noise ratio at the receiver input (jamming-to-signal ratio [J/S]), which is also called jamming coefficient (K). The jamming coefficient means the ratio of jamming noise power (P_{jr}) and signal power (P_{tr}) measured at the receiving point. Jamming is effective if the jamming noise/signal power ratio at the receiver's input is higher than the minimum value of the jamming coefficient (K_{min}).

The jamming coefficient depends primarily on the modulation method. Therefore, the more complex modulation method is used, the higher the J/S ratio is needed for effective jamming.

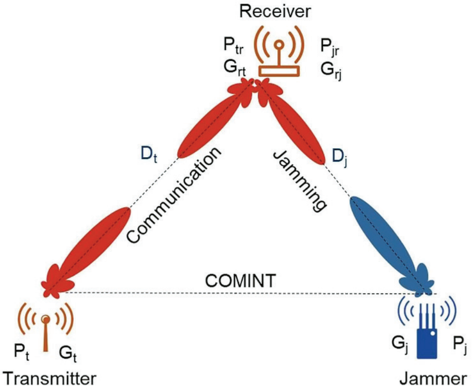


Figure 4: The general geometry of effective jamming of radio communication networks
Source: Compiled by the authors.

The effectiveness of electronic jamming of radio communication networks depends on the following factors:

- power of communication transmitter (P_t)
- gain of transmitter antenna towards receiver (G_t)

[8] Sándor Gyányi: Informatikai WLAN-hálózatok zavarása. *Bolyai Szemle,* 18, no. 4 (2009). 119–132.

- gain of receiver antenna towards transmitter (G_{rt}) and towards jamming source (G_{rj})
- jamming signal power (P_j)
- gain of jammer antenna towards receiver (G_j)
- distance between transmitter and receiver (absorption loss) (D_t)
- distance between jammer and receiver (absorption loss) (D_j)
- bandwidth of jamming signal (Δf_j) and receiver's effective adjacent channel rejection
- mode of the applied modulation (interference tolerance, signal processing) and modulation of jamming signal
- carrier frequency, bandwidth and other factors that have an impact on wave delegation[9]

It is practical to align the jamming signal to the applied modulation from an effective jamming perspective. Thus, the modulation should be regarded as reconciled. In addition, especially in WLAN networks, the receiver antenna gain is the same both towards the transceiver and the jamming unit in practice because these mainly use circular broadcast antennas. Considering these factors, by knowing K_{min} and the main technical and location parameters, after some simplifications, the power required for jamming can be calculated by using the following formula:[10]

$$P_j = K_{min} \frac{P_t G_t D_j^2 \Delta f_j}{G_j D_t^2 \Delta f_r} \qquad [1]$$

where:
P_j – minimum jamming power
P_t – transmitter power
G_t – gain of transmitter
G_j – gain of jammer antenna
D_t – distance between transmitter and receiver
D_j – distance between jammer and receiver
Δf_j – jamming signal bandwidth
Δf_r – receiver's effective adjacent channel rejection
The jamming distance can be calculated by rearranging the formula above:[11]

$$D_j = D_t \sqrt{\frac{P_j G_j \Delta f_r}{K_{min} P_t G_t \Delta f_j}} \qquad [2]$$

[9] Zsolt Haig et al.: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 80.

[10] Haig et al. (2014): op. cit. 81.

[11] Haig et al. (2014): op. cit. 81.

From this it is evident that the effectiveness of jamming primarily depends on the distance, the antenna gain, the power conditions, the jamming-to-signal ratio and the modulation-dependent jamming coefficient. Bandwidth is also an important parameter, especially in broadband jamming, which requires significant jamming power.

There are different jamming types against communication systems. Figure 5 illustrates these types.

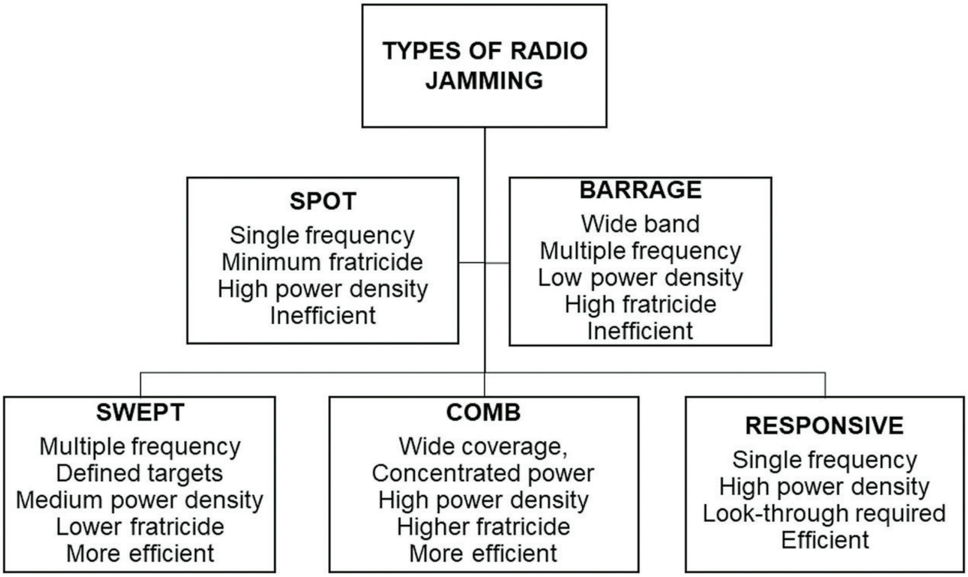


Figure 5: Types of radio jamming

Source: Michael R. Frater – Michael Ryan: Electronic Warfare for the Digitized Battlefield. London– Norwood, Artech House, 2001.

The two basic and longest-used jamming types are spot and barrage. The spot is single-channel jamming, using high power density per single channel. However, because of its low capacity, it has low effectiveness (it only jams a single channel). The barrage is the opposite of the spot. It can jam multiple channels simultaneously on broadband. However, its power density decreases proportionally to bandwidth. Swept and comb combine the advantages of these. The swept in broadband continuously sweeps across the jamming signal with high speed (for example, in the receiver's input bandwidth). As a result, it can be considered spot jamming at each discrete time. On the other hand, the fast frequency sweeping makes it possible to jam multiple channels. In the case of comb jamming, the jammer, which has a pre-programmed list of channels, simultaneously jams the targeted channels, for example, by utilising Frequency Divison Multiple Access (FDMA). The most effective and most challenging to implement jamming is responsive jamming. The receiver of the jammer of this type of jamming continuously scans the bandwidth. Where it finds a jammable channel, there it begins to transmit a jamming signal.

4. Possible ways of jamming WLANs in the physical layer

When jamming WLAN networks, the aim is to deny the communication between the access points (AP) and the connected Wi-Fi devices. Wi-Fi jamming can be implemented in the physical layer by applying the previously introduced radio jamming techniques individually or combined. Another option is to implement jamming in the MAC sublayer, called a protocol-stack attack or protocol-aware attack by the professional literature.[12]

APs or the devices connected to the AP can be targeted by jamming. When APs are targeted, the whole WLAN network becomes inoperable. The user devices cannot connect to the AP, and the network communication discontinues. This can be regarded as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack on the physical layer. When individual WLAN devices are attacked, the receiver is targeted using different methods. This does not result in the overall discontinuation of the Wi-Fi network communication. In the following, the paper reviews the most typical attack methods in the physical layer, using the taxonomy of Pirayesh and Zeng primarily.[13]

The key to physical layer jamming is the relations between jamming signals and useful signal power ratios. The radiated power of the outdoor APs, depending on the applied frequency band, is 23–30dBm (200–1,000mW) on average. This power makes possible a 5–15 km range.[14]

Indoor APs usually use less power. These devices might have 10–20 dBm (10–100 mW) power.

Contrary to these APs, the commercial jammers have 1–10 W (30–40 dBm) total power, but also there is some 100 W (50 dBm) jammer on the market. These devices are usually multi-channel devices (e.g. Wi-Fi, 2G, 3G, 4G, 5G, GPS).[15]

Both the receiver (AP) and the jammer use circular broadcast antennas. Therefore, based on the power parameters, it is evident that it is possible to achieve more than 10–100 times J/S values.

This is true even if most of these jammers apply basic barrage jamming. As a result, it is possible to jam from greater distances (even from hundreds of meters). In the following, the paper summarises the most typical jamming methods.

High-power, continuous, broadband jamming: This type aims to deny access to the channel and packet reception. Measurements proved that 100% packet loss could be achieved in the case of an indoor AP using approximately 100 mW power and 4 dB (~2.5 times) J/S.[16]

Responsive jamming: When packets are detected, a jamming signal is transmitted. This is an effective jamming method because there is no continuous jamming signal

[12] Marc Lichtman et al.: A Communications Jamming Taxonomy. *IEEE Security and Privacy,* 14, no. 1 (2016). 47–54.

[13] Hossein Pirayesh – Huacheng Zeng: *Jamming Attacks and Anti-Jamming Strategies. Wireless Networks: A Comprehensive Survey.* 2021.

[14] CPE220 2,4 GHz-es 300 Mb/s 12 dBi Kültéri Egység. *TP-Link,* s. a.

[15] WiFi Jammer Bluetooth Signals Blocker. *Perfect Jammers,* s. a.

[16] Pirayesh–Zeng (2021): op. cit.; T. Karhima et al.: IEEE 802.11b/g WLAN Tolerance to Jamming. *IEEE MILCOM 2004. Military Communications Conference,* 3 (2004). 1364–1370.

transmission, only when communication is in the channel. The difficulty lies in the short response time. An OFDM symbol time is 4 µs, within which one needs to detect the package and transmit the jamming signal, for example. This makes a rigorous time correlation necessary.[17]

Spoofing (disguising a communication or identity): Sending many seemingly authentic data packets to the AP or a Wi-Fi device. With these data packets, spoofing exhausts the resources of the receiver. The target receives, processes spoofed data and has no remaining resources to process legitimate communication. It shows the effectiveness of spoofing that a low-yield jammer can exhaust all resources of an AP.[18]

Random and periodic jamming: The jammer transmits a jamming signal at random times and is dormant for the remaining time. During periodic jamming, the jamming signal is transmitted at pre-defined periods. It is easier to detect the latter because the jamming follows a predictable pattern. Random and periodic jammers have better energy efficiency because they do not transmit continuously. At the same time, data packet loss is less compared to continuous broadband jamming.[19]

Sweep jamming: In this case, the jammer seeps the overall band with high speed (within less than 10 µs), i.e. it keys up its transmitter from frequency to frequency. Measurements prove that it can reach more than 66% capacity loss in the 2.4 GHz band due to the excellent power density.[20] Its main limit is the need for a quick re-keying sweep jammer. One magnitude higher sweep in the 5 GHz band is necessary than in the 2.4 GHz band because the keyable bandwidth is 10 times larger.

5. Implementing electronic jamming in the physical layer

The authors tested three jamming types in a lab environment introduced previously. A USRP B200 SDR device was used as a jammer. The SDR can operate a full-duplex mode between 70 MHz and 6 GHz in 56 MHz bandwidth. Due to its open-source driver, it is possible to adapt it to many platforms. The GNU Radio application in the Windows environment was selected to control the device from the possible options. The tests were performed in the 2.4 GHz WLAN band.

The test was performed in an interference-free environment, with no other APs operating nearby. The jammer, the transmitter and the receiver were 10 m from each other. 2 dBi gain circular broadcast antennas were used in all test devices. In the GNU Radio application, the output power was set to 100 mW (20 dBm) during the measurement.

[17] Pirayesh–Zeng (2021): op. cit.; Yifeng Cai et al.: Joint Reactive Jammer Detection and Localization in an Enterprise WiFi Network. *Computer Networks,* 57, no. 18 (2013). 3799–3811.

[18] Pirayesh–Zeng (2021): op. cit.; Ioannis Broustis et al.: FIJI: Fighting Implicit Jamming in 802.11 WLANs. In Yan Chen – Tassos D. Dimitriou – Jianying Zhou (eds.): *Security and Privacy in Communication Networks. SecureComm 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.* Volume 19. Berlin–Heidelberg, Springer, 2009.

[19] Pirayesh–Zeng (2021): op. cit.

[20] Suresh Bandaru: Investigating the Effect of Jamming Attacks on Wireless LANs. *International Journal of Computer Applications,* 99, no. 14 (2014). 5–9.

To ascertain the adequate operation of the jammer, a spectrum analyser was used in the test environment to evaluate the radio spectrum before, during and after jamming. Figure 6 illustrates the test environment.

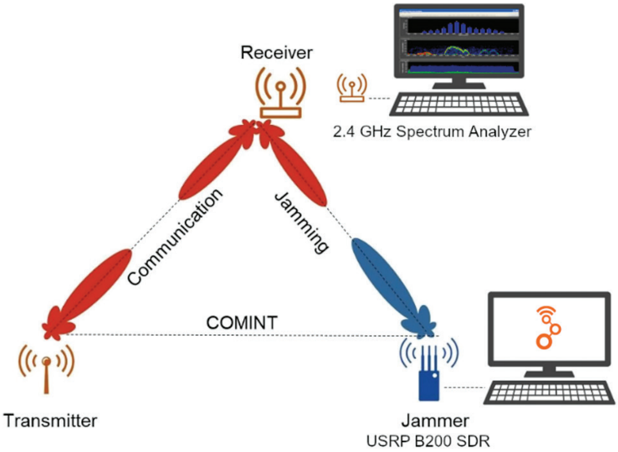


Figure 6: Network configuration for electronic jamming

Source: Compiled by the authors.

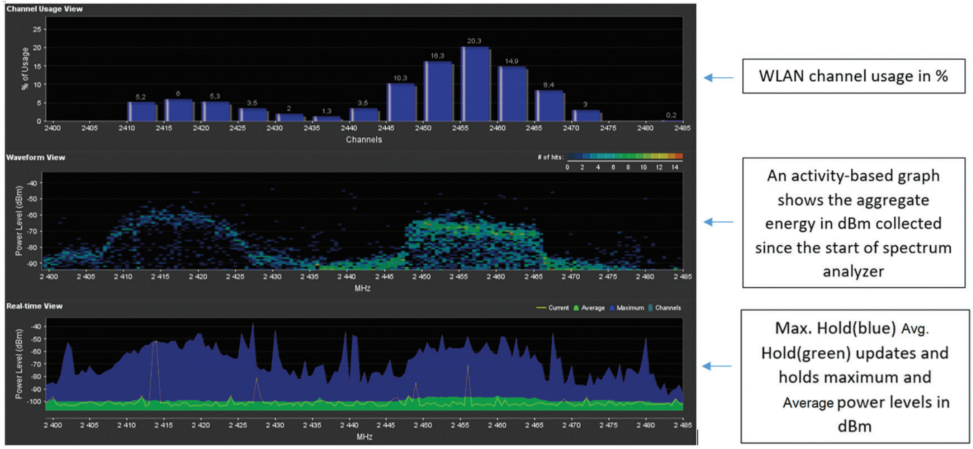
The 2.4 GHz WLAN frequencies and channels should be known to set up the jammer properly. This is summarised in the following table.

Table 4: 2.4 GHz WLAN Band channel numbers and frequencies

Channel Number	**Lower Frequency**	**Center Frequency**	**Upper Frequency**
	MHz	**MHz**	**MHz**
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483

Source: Compiled by the authors based on Wi-Fi Channels, Frequencies, Bands & Bandwidths. Electornics Notes, s. a.

Before the experiment, the radio status of the environment was tested by the spectrum analyser in the 2.4 GHz WLAN band. The spectrum snapshot indicates that two devices broadcasted in the test band. Based on the mid-frequencies, the first AP was on channel 2 (2417 MHz), and the second device was on channel 10 (2457 MHz). Figure 7 shows the spectrum state before the test.



WLAN channel usage in %

An activity-based graph shows the aggregate energy in dBm collected since the start of spectrum analyzer

Max. Hold(blue) Avg. Hold(green) updates and holds maximum and Average power levels in dBm

Figure 7: The 2.4 GHz WLAN spectrum before the tests
Source: Compiled by the authors.

The following figure summarises the J/S (Jamming-to-Signal) value per WLAN channel before the test.

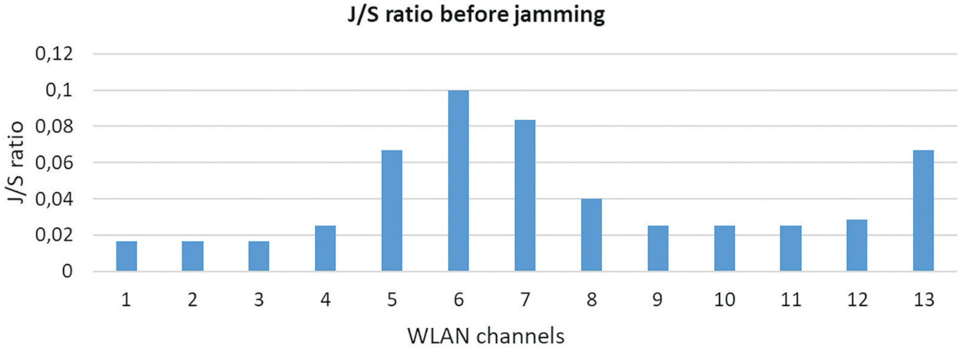
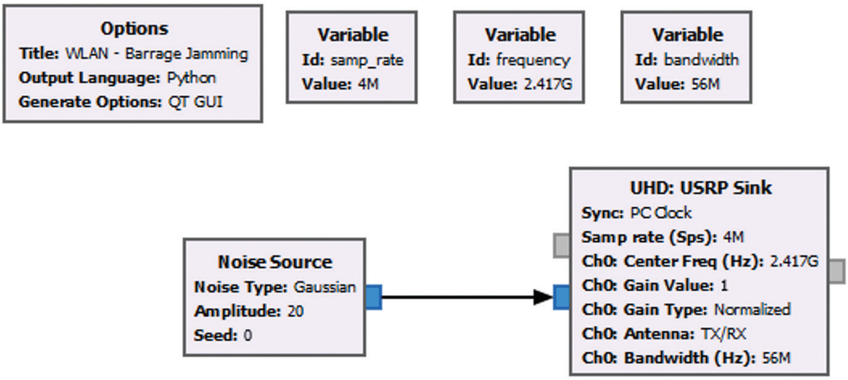


Figure 8: J/S value per the 13 WLAN channels before the test
Source: Compiled by the authors.

The low J/S values represent that the 2.4 GHz band is practically noise-free at the starting point. The connection between the devices is error-free.

5.1. Broadband barrage jamming

A Gauss noise signal was selected and configured in the GNU Radio application to implement the jammer. Channel 2 frequency was set as mid-frequency. Figure 9 shows the block structure built in the application.



Options
Title: WLAN - Barrage Jamming
Output Language: Python
Generate Options: QT GUI

Variable
Id: samp_rate
Value: 4M

Variable
Id: frequency
Value: 2.417G

Variable
Id: bandwidth
Value: 56M

Noise Source
Noise Type: Gaussian
Amplitude: 20
Seed: 0

UHD: USRP Sink
Sync: PC Clock
Samp rate (Sps): 4M
Ch0: Center Freq (Hz): 2.417G
Ch0: Gain Value: 1
Ch0: Gain Type: Normalized
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 56M

Figure 9: The block scheme of barrage jamming in the GNU Radio application
Source: Compiled by the authors.

Taking advantage of the available options of the SDR device, the 56 MHz bandwidth was selected. The emitted jamming power was 100 mW (20 dBm). The radio spectrum was analysed during the run of the jammer. Figure 10 shows this spectrum image.

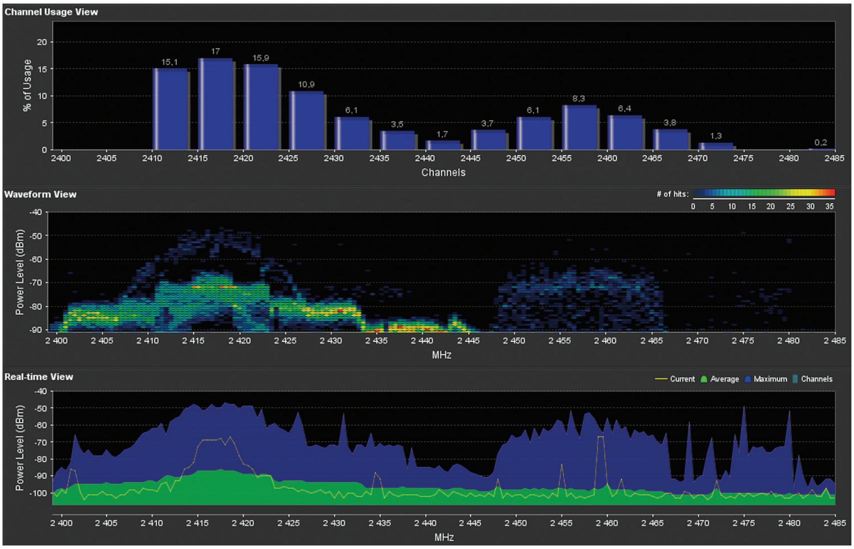


Figure 10: The effect of barrage jamming on the 2.4 GHz WLAN spectrum
Source: Compiled by the authors.

The spectrum image illustrates that the jamming signal of the barrage affects the overall WLAN spectrum. The top segment of the figure shows the channel load. This indicates that the main load was on channel 2. The middle segment of the figure shows the spectrum image varying from the more active to the less active values in red to blue. The drawn-out-shape of the jamming stands out in this image. The bottom segment of the figure indicates the minimum and maximum values of the signal. Here the signal and jamming are mixed. The spectrum image shows that jamming on the centre frequency was –65 dBm RSSI, and the average emitted frequency was –75 dBm. Due to jamming, the transmission signal of the device on channel 2 is not significant. The following figure shows the J/S value projected to the WLAN channels during barrage jamming.

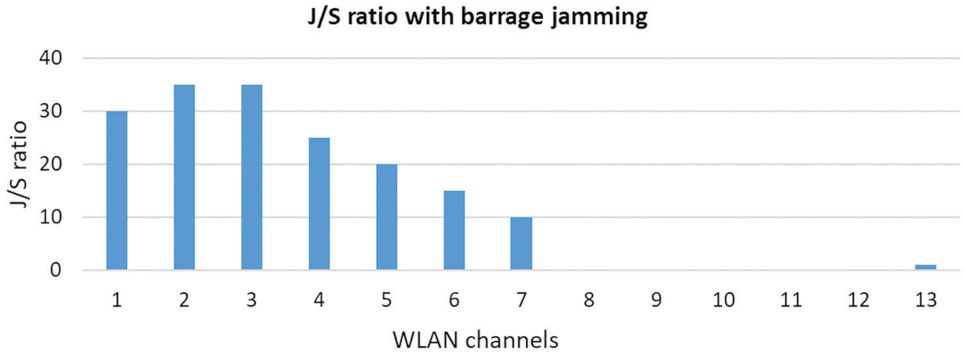
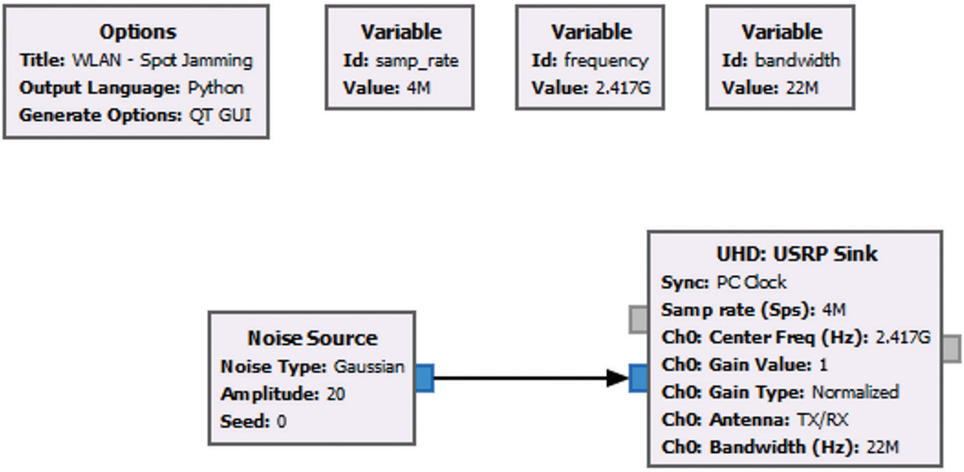


Figure 11: J/S value projected to the 13 WLAN channels during barrage jamming
Source: Compiled by the authors.

This jamming affects the first seven channels. The peak is on channels 2 and 3. The J/S value here was 45. The objective of this test was to jam the communication between devices using channel 2. As a result of this jamming, devices were unable to establish communication. The loss was 100%.

5.2. Spot jamming

The objective of this test was to deny the communication of devices using channel 2, but with spot jamming on the 22 MHz bandwidth. The bandwidth was selected because the bandwidth of an effective WLAN channel is closely 22 MHz. The jamming bandwidth is the same as the signal bandwidth in spot jamming. The jamming mid-frequency was set to 2417 MHz in this case. For the implementation, the previously implemented structure was used. This is illustrated in Figure 12.



Options
Title: WLAN - Spot Jamming
Output Language: Python
Generate Options: QT GUI

Variable
Id: samp_rate
Value: 4M

Variable
Id: frequency
Value: 2.417G

Variable
Id: bandwidth
Value: 22M

Noise Source
Noise Type: Gaussian
Amplitude: 20
Seed: 0

UHD: USRP Sink
Sync: PC Clock
Samp rate (Sps): 4M
Ch0: Center Freq (Hz): 2.417G
Ch0: Gain Value: 1
Ch0: Gain Type: Normalized
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 22M

Figure 12: The block scheme of spot jamming in the GNU Radio application
Source: Compiled by the authors.

The radio spectrum was analysed during the operation of the jammer. Figure 13 shows this spectrum image.

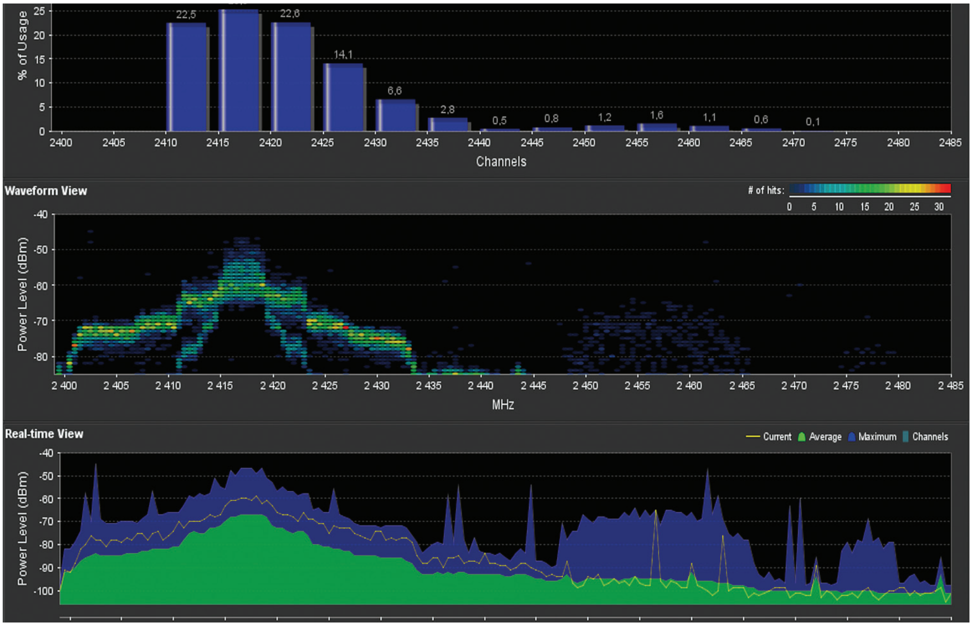


Figure 13: Spot jamming spectrum image on WLAN channel 2
Source: Compiled by the authors.

The image shows that the jamming primarily affects channel 2. On the mid-frequency of the channel, the jamming signal is –50 dBm RSSI. As a result of spot jamming, the transmission signal of the device on channel 2 is not significant. The following figure shows the J/S value projected to the WLAN channels during spot jamming.

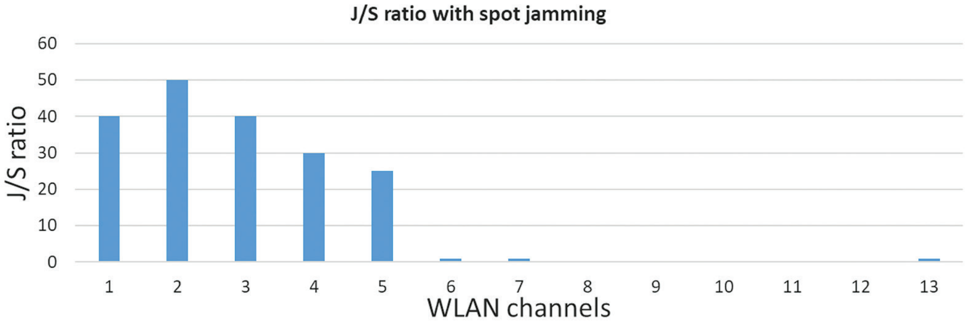
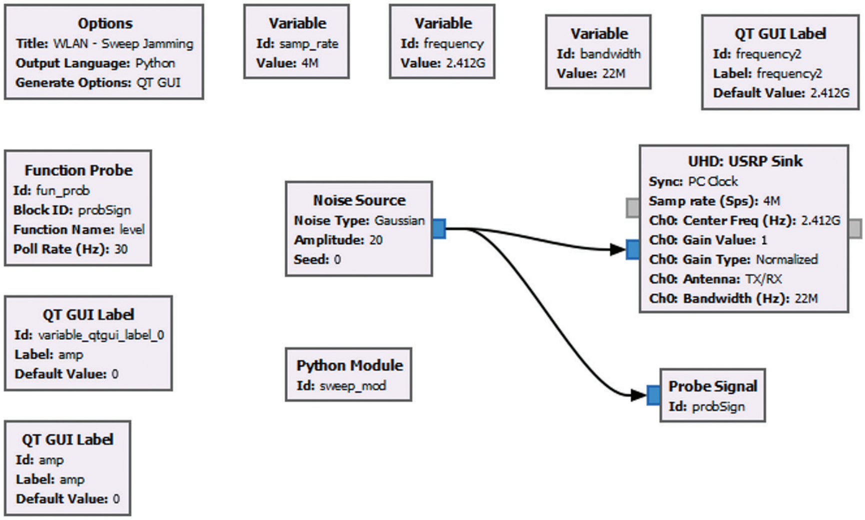


Figure 14: J/S value projected to the 13 WLAN channels during spot jamming
Source: Compiled by the authors.

This jamming affects the first five channels. The peak is in channel 2. The J/S value here was 55. The objective of this test was to jam the communication between devices using channel 2. As a result of this jamming, devices were unable to establish communication. The loss was 100%.

5.3. Sweep jamming

The start and end frequencies and the forward steps had to be determined during this test. From the frequency table, the centre frequencies were selected. The forward steps were set to 5 MHz. In the GNU Radio application, the sweep function was implemented by a custom-made Python code. This application defined the frequency values for the blocks in each step. Figure 15 shows the block level structure of this automated solution.



Options
Title: WLAN - Sweep Jamming
Output Language: Python
Generate Options: QT GUI

Variable
Id: samp_rate
Value: 4M

Variable
Id: frequency
Value: 2.412G

Variable
Id: bandwidth
Value: 22M

QT GUI Label
Id: frequency2
Label: frequency2
Default Value: 2.412G

Function Probe
Id: fun_prob
Block ID: probSign
Function Name: level
Poll Rate (Hz): 30

Noise Source
Noise Type: Gaussian
Amplitude: 20
Seed: 0

UHD: USRP Sink
Sync: PC Clock
Samp rate (Sps): 4M
Ch0: Center Freq (Hz): 2.412G
Ch0: Gain Value: 1
Ch0: Gain Type: Normalized
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 22M

QT GUI Label
Id: variable_qtgui_label_0
Label: amp
Default Value: 0

Python Module
Id: sweep_mod

Probe Signal
Id: probSign

QT GUI Label
Id: amp
Label: amp
Default Value: 0

Figure 15: The block scheme of sweep jamming in the GNU Radio application

Source: Compiled by the authors.

The bandwidth was set to 22 MHz in this test. The radio spectrum was analysed again during the operation of the jammer. Figure 16 shows the result of this radio spectrum analysis.

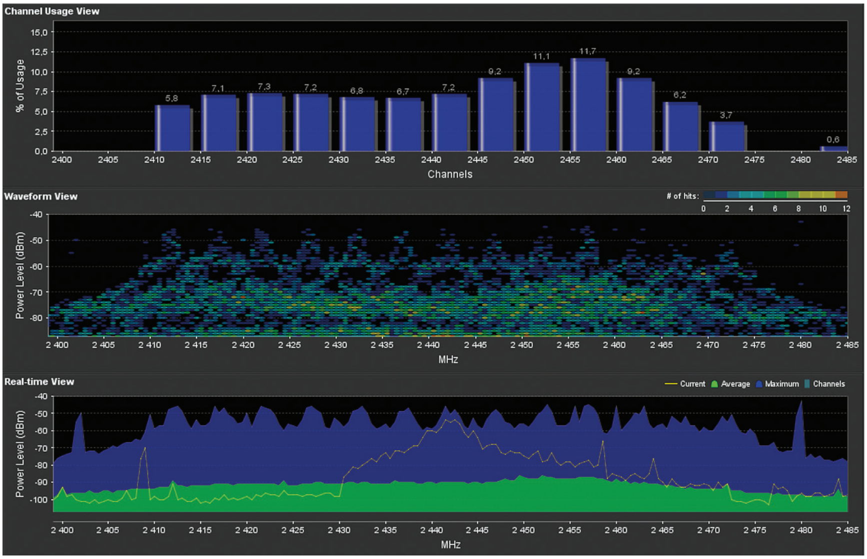


Figure 16: Sweep jamming spectrum image on the overall 2.5 WLAN band

Source: Compiled by the authors.

The following figure shows the J/S value projected to the WLAN channels during sweep jamming.

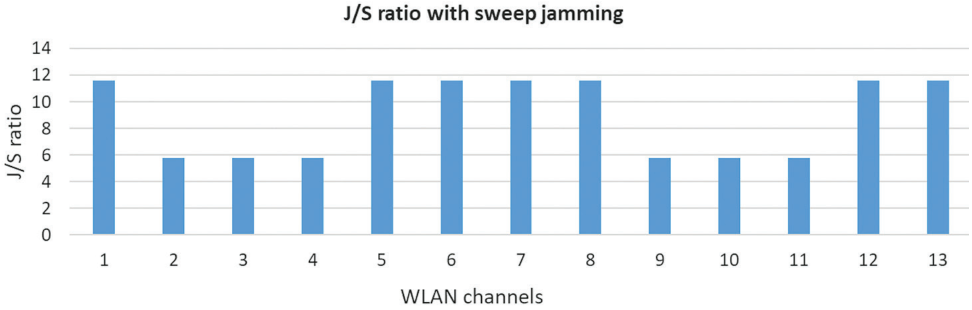


Figure 17: J/S value per the 13 WLAN channels during sweep jamming
Source: Compiled by the authors.

As a result of this test, the networking devices on this channel had a 45% of packet loss. This value was calculated from the up and download speed trends. The J/S ratio was in the range of 5.8 and 11.8 due to jamming. The spectrum image illustrates the jamming effects in the full WLAN band. Still, its intensity is below both spot and barrage jamming.

6. Conclusions

WLAN networks and devices are prone to electronic jamming day after day. In some instances, the applied technology permits jamming to be hidden from users or barely perceptible. Deliberate and targeted jamming, however, can render the communication channel unusable fully or partially for users. This paper summarised the possibilities of jamming WLANs in the physical layer. The paper also provides experimental evidence that the applicable jamming in the physical layer, which is described in theory, can be implemented by anybody with a widely available SDR.

A comparatively low (100 mW) jamming power was used in all cases. From the J/S effectiveness perspective, spot jamming was the best during the tests. It is also notable that jamming does not only affect the targeted channel (channel 2) but also was significant in four neighbouring channels (channels 1, 3, 4 and 5). Falling in all cases, the J/S ratio of spot jamming was above 20. Following the theory, the J/S value during the barrage jamming was lower than in the case of spot jamming. However, this jamming affected seven channels, and falling in all the cases, the J/S ratio of spot jamming was above 10. One of the exciting findings of the tests is that the J/S value is lower for spot jamming than the other two; in this case, the theory suggests that the spectral power density projected to 22 MHz is better than 56 MHz bandwidth barrage. However, these J/S values were sufficient to classify the jamming as effective.

The tests ascertained that the data loss in channel 2 was 100% due to both barrage and sweep jamming and 45% as a result of sweep jamming.

The experiments also highlighted that there is no need for high jamming power to implement some methods to deny communications effectively in WLANs if the jammers are close enough to the target devices. Of course, higher power is needed to jam from greater distances or implement jamming from an external source in all the tested methods. Based on theoretical calculations and causations, the smaller jamming distance reduces the required adequate jamming power by the square root, which means that in the case of half distance between the jammer and the target, only 1/4th of jamming power is sufficient. Of course, this works both ways. Twice the distance between the jammer and the target requires four times higher jamming power. This paper highlighted the vulnerability of contemporary WLAN networks in the physical layer, which could cause a severe cybersecurity issue and should be considered, especially in critical infrastructures.

References

Bandaru, Suresh: Investigating the Effect of Jamming Attacks on Wireless LANs. *International Journal of Computer Applications,* 99, no. 14 (2014). 5–9. Online: https://doi.org/10.5120/17439-8180

Bhardwaj, Rashmi: Wi-Fi generation comparison Wifi6 vs Wifi5 vs Wifi4. *Network Interview,* s. a. Online: https://networkinterview.com/wi-fi-generation-comparison-wifi6-vs-wifi5-vs-wifi4/

Broustis, Ioannis – Konstantinos Pelechrinis – Dimitris Syrivelis – Srikanth V. Krishnamurthy – Leandros Tassiulas: FIJI: Fighting Implicit Jamming in 802.11 WLANs. In Yan Chen – Tassos D. Dimitriou – Jianying Zhou (eds.): *Security and Privacy in Communication Networks. SecureComm 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Volume 19. Berlin–Heidelberg, Springer, 2009. Online: https://doi.org/10.1007/978-3-642-05284-2_2

Cai, Yifeng – Konstantinos Pelechrinis – Xin Wang – Prashant Krishnamurthy – Yijun Mo: Joint Reactive Jammer Detection and Localization in an Enterprise WiFi Network. *Computer Networks,* 57, no. 18 (2013). 3799–3811. Online: https://doi.org/10.1016/j.comnet.2013.09.004

CPE220 2,4 GHz-es 300 Mb/s 12 dBi Kültéri Egység. *TP-Link,* s. a. Online: www.tp-link.com/hu/business-networking/outdoor-radio/cpe220/

Danel, Eve: Wi-Fi 6's OFDMA Challenges Make Verification Crucial. *RF Globalnet,* 02 December 2019. Online: www.rfglobalnet.com/doc/wi-fi-s-ofdma-challenges-make-verification-crucial-0001

Frater, Michael R. – Michael Ryan: *Electronic Warfare for the Digitized Battlefield.* London– Norwood, Artech House, 2001.

Gyányi, Sándor: Informatikai WLAN-hálózatok zavarása. *Bolyai Szemle,* 18, no. 4 (2009). 119–132.

Haig, Zsolt – László Kovács – László Ványa: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Karhima, T. – A. Silvennoinen – M. Hall – S.-G. Haggman: IEEE 802.11b/g WLAN Tolerance to Jamming. *IEEE MILCOM 2004. Military Communications Conference,* 3 (2004). 1364–1370. Online: https://doi.org/10.1109/MILCOM.2004.1495141

Lichtman, Marc – Jeffrey D. Poston – Saidhiraj Amuru – Chowdhury Shahriar – T. Charles Clancy – R. M. Buehrer – Jeffrey H. Reed: A Communications Jamming Taxonomy. *IEEE Security and Privacy,* 14, no. 1 (2016). 47–54. Online: https://doi.org/10.1109/MSP.2016.13

McKee, Caleb: *OFDMA vs OFDM explained.* 04 March 2021. Online: www.minim.com/blog/what-is-wifi-6-ofdma-vs-ofdm-explained

Pirayesh, Hossein – Huacheng Zeng: *Jamming Attacks and Anti-Jamming Strategies. Wireless Networks: A Comprehensive Survey.* 2021. Online: https://doi.org/10.1109/COMST.2022.3159185

QAM modulator and demodulator. *Faststream Technologies,* 28 February 2022. Online: https://faststreamtechblogs.wordpress.com/2022/02/28/qam-modulator-and-demodulator/

Signal-to-Noise Ratio (SNR) and Wireless Signal Strength. *CISCO,* s. a. Online: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength

What is WiFi Strength and RSSI? *SimpliSafe,* s. a. Online: https://support.simplisafe.com/hc/en-us/articles/360035742191-What-is-WiFi-Strength-and-RSSI-

Wi-Fi 4/5/6/6E (802.11 n/ac/ax). *Duckware,* 03 September 2022. Online: www.duckware.com/tech/wifi-in-the-us.html

Wi-Fi Channels, Frequencies, Bands & Bandwidths. *Electornics Notes,* s. a. Online: www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php