sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 3 2020

WI-FI JAMMING USING SOFTWARE DEFINED RADIO

Annamaria SÂRBU, Dumitru NEAGOIE

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
paljanosanna@yahoo.com

Abstract: *In this article we present software defined radio (SDR) instrumentation used for interfering or jamming Wi-Fi networks. A Wi-Fi network analyzer application was used together with a low cost, commercially available SDR, Hack RF one, to conduct aimed interference on a 802.11 b/g/n network. A GNU radio flowchart was used to control the radio transceiver (SDR) by emitting a jamming signal aimed towards the targeted client by means of a directional antenna. Various signal bandwidths and distance from the targeted device were tested to characterize the adequate parameters of an effective jamming signal with respect to the calculated signal to noise ratio (SNR). Jamming efficiency was evaluated by means of a Wi-Fi connectivity speed test application installed on the targeted device, in order to measure connectivity degradation if complete jamming was not possible. Results presented suggest that Wi-Fi jamming is possible by means of SDR technology, providing insights on the methodology used and initial optimisation procedures in the test environment.*

Keywords: software defined radio, Wi-Fi, network performance, jamming, SNR

1. Introduction

Wi-Fi networks are widely available nowadays, becoming an important part of communication planning essential for both general public LAN's and professional communication networks. Data transfer performance and range are of primarily interest when setting up a Wi-Fi environment. However, security issues related to the use of these networks have been a subject of wide interests among both users and researchers, as their functionality becomes vital in sensitive domains like healthcare or defence. [1, 2]

Radio jamming represents the action of deliberate electromagnetic emission for blocking or interference over an authorized radio communication. A wide variety of sensitive devices like drones, health monitor sensors or surveillance cameras rely on Wi-Fi communication. Public literature gives little information on Wi-Fi jamming attacks and how they could be conducted [3, 4]. To this extent, in [3] authors demonstrate that 802.11 wireless LANs are vulnerable to selective jamming attacks and propose judicious use of randomization to address the problem. Physical layer attacks are also presented in [4] contributing to phenomenon characterization of filed propagation within the wireless spectrum.

Software defined radio (SDR) devices are low cost transceivers that became widely available on the market. Generally, they can be controlled by open source software enabling infinite possibilities for both researchers and people with malicious intentions. In [5] the author presents some unpublished results regarding the use of a USRP B210 SDR for Wi-Fi jamming. The results focus on jamming effect on delay time for different output power configuration. The literature review so far

DOI: 10.2478/kbo-2020-0132

shows little knowledge of the jamming effect on user perceived quality of service or signal parameters. The objective of this article is to provide a more depth analysis of the jamming effect for different configuration signals emitted by Hack RF [6], a commercially available SDR. The user perceived quality of service (Wi-Fi upload/download speed) for a device under test (DUT) was measured using an available android application and plotted versus the calculated signal to noise ratio (SNR). The following sections will describe the materials and methods used, the results, discussions and conclusions of this work.

2. Materials and methods

A. Experimental setup

The Wi-Fi network was set up by means of a router model Tp Link Archer C6, which is a dual-band wireless router equipped with 4 antennas. A Huawei P10 Lite mobile phone was used as the targeted device (DUT) for the jamming experiments. Only 802.11 b/g/n standard jamming was experimented, with the router set on channel 2 (central frequency 2.417 GHz), high power enabled. Channel bandwidth was chosen to be 20 MHz or 40 MHz, depending on the scenario employed.

The hardware used for jamming was HackRF, a very low cost (350$) SDR, equipped with a directive antenna model Aaronia Hyper Log 7060. GNU Radio Companion (GRC) software environment was used for modelling the Hack RF transmission. In the GRC flowchart, the HackRF sample rate was set to 20 MHz, and a noise source block was applied to an Osmocom Sink (HackRF) block emitting on the Ch2 central frequency.

The experiments were carried out in an indoor laboratory where both wireless router and DUT were positioned in a fixed position. This ensured the same received signal strength at the DUT location. The DUT was placed on a wooden tripod at 1,1 m above the floor. The directive antenna connected to the SDR hardware was also placed on a wooden tripod at the same height as the DUT. 19 points were measured with the antenna being placed away from the DUT by various distances between 10 and 400 cm. Figure 1 presents the experimental setup.

Figure 1: Experimental setup

Three measurement scenarios were considered:

1. Router with high emission power configured on channel 2 with 20 MHz bandwidth and SDR configured with 20 MHz bandwidth jamming noise signal
2. Router with high emission power configured on channel 2 with 40 MHz bandwidth and SDR configured with 20 MHz bandwidth jamming noise signal
3. Router with high emission power configured on channel 2 with 40 MHz bandwidth and SDR configured with 10 MHz bandwidth jamming noise signal

B. Network performance measurement

In order to test the effect of the jamming signal on the Wi-Fi network performance, the upload and download speeds were measured with the free Wi-Fi Speed Test android application [7]. A network consisting of a Wi-Fi connected DUT (mobile phone) and a local TCP server was configured according to figure 2a. The installed application (figure 2b) was then used to test the Wi-Fi upload and download speed using TCP protocol by sending/receiving 10 Mb of data to the computer. In order to avoid interference and test the effect of the jamming signal on a

sole device only the computer was connected via an Ethernet cable to the wireless router.

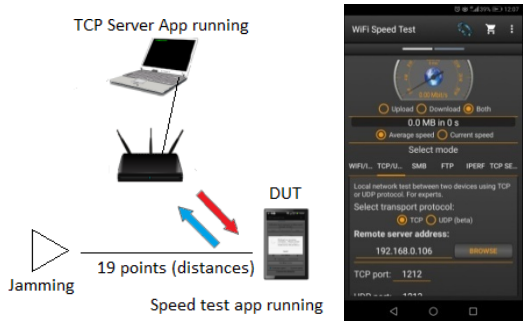

Figure 2 a: Network topology
b. Wi-Fi Speed Test application interface

Speed measurements were conducted in the presence of the jamming signal. Different distances between the DUT and the jammer were tested.

C. Signal to noise ratio (SNR) calculation

The output signal power of the SDR used for jamming was measured by a R&S FSL spectrum analyzer. Hack RF emitted channel bandwidth was varied between 20 MHz and 10 MHz occupied bandwidth as measured by the spectrum analyzer (SA). The channel power of the applied signal was measured in the 20 MHz or 40 MHz targeted bandwidth (figure 3).

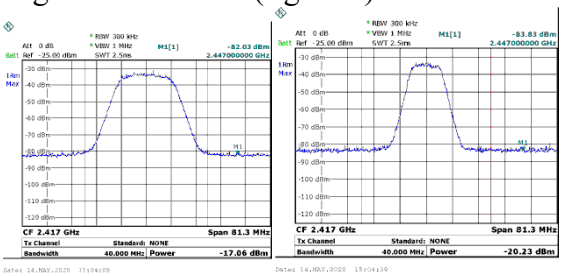

Figure 3:Channel power measurement for HackRF emission in the 40 MHz Wi-Fi channel
a. 20 MHz bandwidth jamming signal
b. 10 MHz bandwidth jamming signal

Moreover the VSWR of the antenna used for jamming was measured by means of a Voltage Standing Wave Ratio (VSWR) meter in order to count for any mismatch loss (ML). The measured VSWR was 2.1 at the operating frequency corresponding to 0.58 dB mismatch loss. The antenna gain (AG) was extracted from the gain chart provided by manufacturer (5.1 dBi). The SNR was calculated based on equation (1).

$$SNR[dB] = P_{Wi-fi}[dB] - (P_{SDR}[dB] + AG\ [dB] - ML\ [dB] - FSPL[dB]) \quad (1)$$

Where,

P_{Wi-fi}- represents the Wi-Fi power at the DUT position. This was considered to be the received signal strength indicator (RSSI), as measured by a Wi-Fianalyzer app [8] installed on the DUT (Figure 4)

P_{SDR} - represents the SDR emitted power measured with the SA as the channel power in the band (20/40 MHz)

AG- antenna gain

ML- the mismatch loss

FSPL – Free space path loss calculated based on equation (2)

$$\text{FSPL[dB]} = 20log_{10}(d) + 20log_{10}(f) + 32.44 \quad (2)$$

Where,

d- distance between the DUT and the jamming device antenna [km]

f- frequency of transmission = 2417 MHz

Measurements were performed in a “quiet” Wi-Fi environment with a sole network configured. Both SA and the Wi-FiAnalyzer app installed (Figure 4) confirmed the above statement.

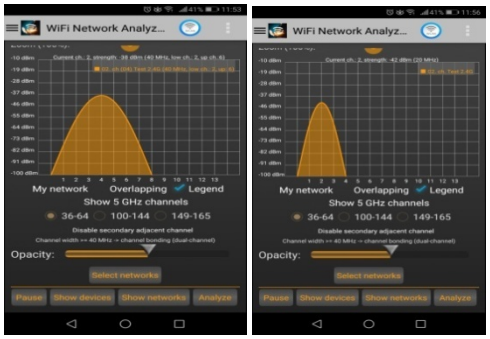

Figure 4: Wi-Fi Analyzer app indicating the enabled Wi-Fi channel width and RSSI

4. Results and discussion

In figure 5 we plotted the upload speed versus the SNR for the three experimental scenarios (description in section 2a).

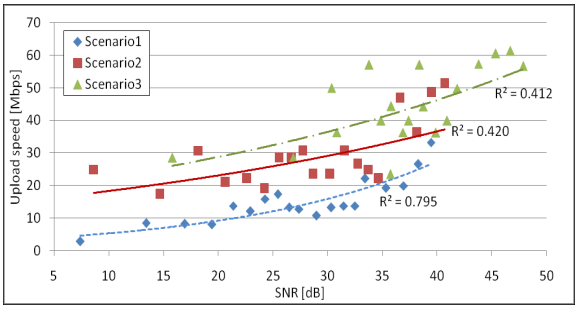

Figure 5: Upload speed versus calculated SNR for the three experimental scenarios

In scenario 1 the ratio of the Wi-Fi channel to the jammed bandwidth was 1/1 while in scenarios 2 and 3 the ratio was of ½ respectively ¼. As expected the bigger this ratio the stronger the effect on the upload speed. From figure 5, one can notice the exponential growth of the upload speed with the increase of the SNR. Exponential trend lines were applied and the corresponding R^2 values were displayed on the chart. Based on the R^2 values, the best fitting curve was obtained for scenario1 when all of the Wi-Fi channel bandwidth was jammed. For upload speeds below 20 Mbps we observed disconnecting of real time applications like VoIP.

The effect of the jamming signal on the measured upload speed was significant.

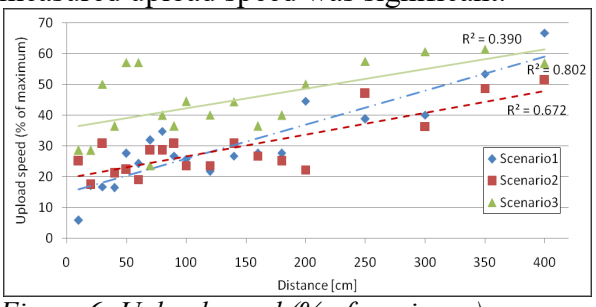

Figure 6: Upload speed (% of maximum) versus jammer distance

In order to express this effect in figure 6 we have plotted the upload speed as percent of the maximum measured upload speed without the presence of the jammer. On the horizontal axis we have plotted the distance of the antenna emitting the noisy signal from the DUT.

One can observe that even if only ¼ of the Wi-Fi Channel bandwidth was jammed the upload speed was reduced by values between 70% and 40% depending on the distance between the jammer and the DUT. The reduction was even more significant for scenarios 1 and 2. So, even if not completely interrupted the communication between the DUT and router was seriously interfered with.

In figure 7 we have plotted the download speed versus the SNR for the three experimental scenarios.

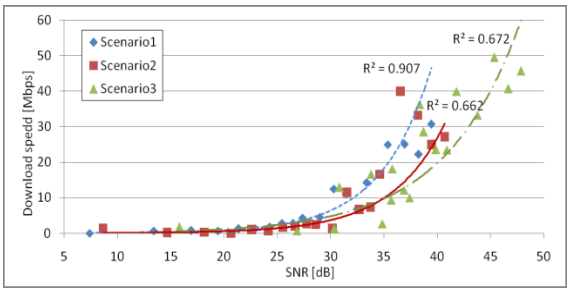

Figure 7: Download speed versus calculated SNR for the three experimental scenarios

As compared to the measured upload speed one can observe from figure 7 that the measured download speed was much lower. We have obtained values below 10 Mbps for SNR values of up to 35 dB. Below 35 dB of SNR, applications like video streaming or other resource consuming were interrupted. Additionally, the trend line exhibits a more exponential character, as higher values of R^2 were calculated.

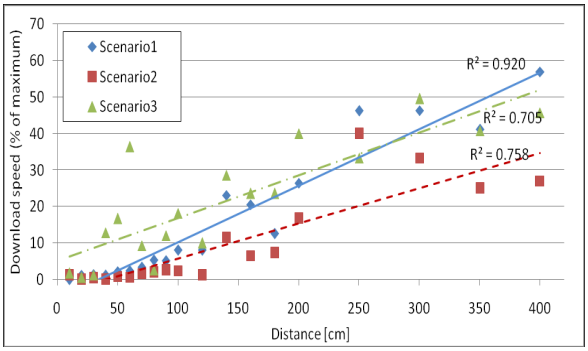

Figure 8: Download speed (% of maximum) versus jammer distance

From figure 8 we can observe the degradation of the download speed (as percentage of the maximum download speed measured without the presence of the jammer) with distance. At distances below 1m we can observe that the degradation is

severe as download speeds are drastically affected. Degradation is less visible as distance increases but even at distances of 4m we can observe that the download speed was halved, seriously affecting network performance and user perceived quality of service. Download speed was observed to be more affected as compared to upload speed by the presence of the jamming signal. The observed results could be explained by the experimental setup which involved client jamming, with router positioned at 3-8 m from DUT in the antenna radiation beam.

Before jumping to conclusions, we have to make one more observation. The signal emitted by the SDR was configured to be of IF gain 20 out of a maximum of 40. An increase of power of 20 dB is possible for the jamming signal. This will lead to lowering the SNR even more at the considered distances.

5. Conclusions

In this article we have proven the vulnerabilities of a Wi-Fi network facing physical layer jamming. We have demonstrated that by means of a commercially, low cost SDR, Wi-Fi jamming can be obtained, providing information about the distances and SNRs required to obtain a specific performance degradation. In situations when data rate are extremely important, the type of jamming presented here could create connectivity problems and seriously affect the user perceived quality of service even when jammer is placed at considerable distance from the targeted device.

With nowadays SDRs becoming much more available and small dimensioned, specialist should consider further security issues related to the use of Wi-Fi network in critical domains like healthcare or defence.

Further research in this area includes testing different router configurations and Wi-Fi standards (eg. 802.11ac) in the 5 GHz band and developing an adaptive jamming algorithm.

References

[1] Bednarczyk Mariusz, Piotrowski Zbigniew, *Will WPA3 really provide Wi-Fi security at a higher level?*, Proceedings of SPIE, Volume: 11055, DOI: 10.1117/12.2525020, Oltarzew, Poland, November, 2019

[2] MekhazniaTahar, Zidani Abdelmadjid, *Wi-Fi security analysis,* Proceedings of the International Conference on Advanced Wireless Information and Communication Technologies (AWICT 2015),Vol.73, pp. 172-178, DOI: 10.1016/j.procs.2015.12.009, Tunisia, 2015

[3] Orakcal Cankut, Starobinski David, *Jamming-resistant rate adaptation in Wi-Fi networks,* Performance Evaluation, Vol. 75-76, pp 50-68, DOI: 10.1016/j.peva.2014.02.002, 2014

[4] Dariusz Czerwiński, Jarosław Nowak*, Field propagation of jamming sources in WiFi networks,* Proceedings of the 2017 International Conference on Electromagnetic Devices and Processes in Environment Protection with Seminar Applications of Superconductors (ELMECO &AoS), DOI: 10.1109/ELMECO.2017.8267715, 2018, Performance Evaluation, Vol. 75-76, pp 50-68, DOI: 10.1016/j.peva.2014.02.002, 2014

[5] García Jorge Alberto Duarte, Software Defined Radio for Wi-Fi Jamming. Unpublished, 2016, https://doi.org/10.13140/RG.2.2.23772.90240

[6] https://greatscottgadgets.com/hackrf/

[7] https://pzoleeblogen.wordpress.com/2013/11/26/wifi-speed-test-for-android-how-to/

[8] https://mobile.softpedia.com/apk/wifi-analyzer-by-zolt-n-pallagi/