2nd URSI AT-RASC, Gran Canaria, 28 May – 1 June 2018

Mitigation Technique to Reduce the Wi-Fi Susceptibility to Jamming Signals

Grecia Romero*(1), Virginie Deniau(2), and Eric Pierre Simon(1)
(1) University of Lille, Villeneuve d'Ascq 59650, France (e-mail: grecia.romero@ed.univ-lille1.fr*)
(2) IFSTTAR, Villeneuve d'Ascq 59650, France (e-mail: virginie.deniau@ifsttar.fr)

Abstract

This paper presents a series of tests that were carried out to characterize a conventional jammer with the aim of identifying the main features of jamming signals. Then, a susceptibility analysis of IEEE 802.11n communications facing the salient identified characteristics of jamming signals is carried out, and a preliminary proposal of a mitigation technique to reduce the susceptibility of IEEE 802.11n communications regarding jamming signals is presented.

1 Introduction

Wi-Fi communications are vulnerable to different types of interference signals [1], including intentional electromagnetic (EM) interference. This type of interference aims to disrupt, confuse or damage electronic systems and/or communication signals through the generation of electromagnetic energy [2, 3]. The generated EM energy levels can be either high power or comparable power to those of the communication signals. In this paper, we focus on the latter case, conventional jammers. These devices are used to degrade network performance by transmitting jamming signals in the frequency band of the target communication network, including Wi-Fi communications.

It is necessary that Wi-Fi communication systems implement mitigation techniques to reduce the impact of these EM jammers on their performance.

The present work describes the main characteristics of the jamming signal in Section 2. Them, in Section 3 a susceptibility analysis of IEEE 802.11n communications is presented. In Section 4, a mitigation technique to reduce the Wi-Fi susceptibility facing jamming signal is presented. Finally, conclusions are presented in Section 5.

2 Characteristics of jamming signals

Jamming signals generated by commercial jammers have been characterized. More specifically, several commercial devices were used in order to compare and identify the main features of jamming signals obtained from these devices.

Table 1 presents characteristics of a commercial jammer regarding the target systems. This jammer covers eight frequency bands, including the 2.4 GHz Wi-Fi band.

Table 1. Commercial jammer characteristics.

Jammer with 8 antennas		
Antenna	**Band (MHz)**	**Type**
1	925-960	2G GSM 900 (Download)
2	1805-1880	2G DSC 1800 (Download)
3	2110-2170	3G UMTS (Download)
4	1570-1580	GPS (1575.42 MHz)
5	2400-2485	Wi-Fi 802.11 b/g/n
6	168-178	Lojack (173.075 MHz)
7	2620-2690	4G LTE (Download)
8	790-862	4G LTE (Upload-Download)

A set of measurements were performed on the different frequency bands of the jammer. However, this paper focuses on the 2.4 GHz band used in Wi - Fi communications. Thus, we present measurement results of the jamming signal generated by output 5 of the jammer, which covers the 2.4 GHz Wi-Fi band according to Table 1.

To identify the exact frequency bands covered by output 5, this output was measured by way of a spectrum analyzer (N9030A PXA signal analyzer 3 Hz - 44 GHz). An attenuator of 30 dB was connected to the spectrum analyzer input. The results of Max Hold traces are displayed in Figure 1. It is observed that the jammer covers the whole range from 2.4 GHz to 2.5 GHz.

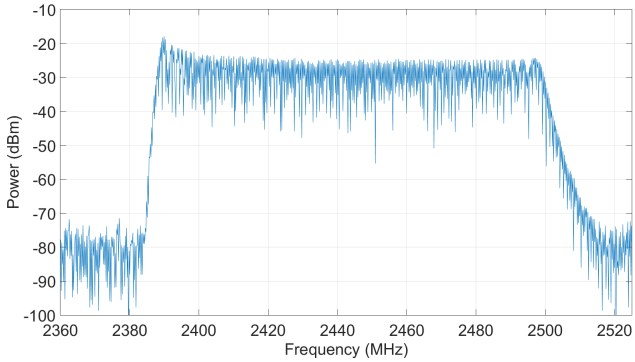

Figure 1. Spectrum representation of the antenna 5 of the commercial jammer (Table 1).

To obtain the Time-Frequency representation, the output signal was measured using an oscilloscope (LeCroy WaveMaster 813Zi-B 13 GHz) with 10 Gsamples/s, including a

30 dB attenuator at the oscilloscope input. Finally, Time-Frequency representations were obtained through spectrogram algorithms applied to the stored data on the oscilloscope.

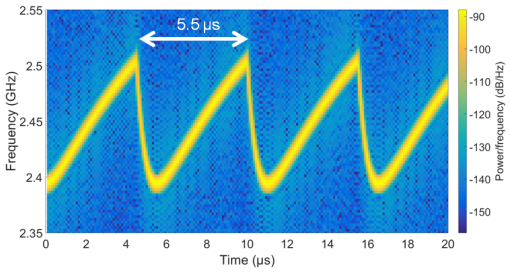

Figure 2. Spectrogram of output 5 of a commercial jammer (Table 1).

Figure 2 shows a Time-Frequency representation of the jamming signal generated by output 5, this signal type is a chirp signal, whose frequency band is swept in time [4]. It is noted that all the other outputs have similar Time-Frequency representations. The time duration to scan the 2.4 GHz band is 5.5 μs. This parameter has the same value for other outputs. Furthermore, by characterizing different jammers, it is observed that the nature of the jamming signals is similar but the time duration to scan the frequency bands can be different from one jammer to another. Thus, we identify this parameter as a key parameter of the jamming signal. This parameters is referred to as *Sweep Period* (SP).

3 Susceptibility analysis of IEEE 802.11n communications as a function of the sweep period

As mentioned earlier, the sweep period or SP is a key parameter of jammers and it is independent of the frequency band to cover. A study of IEEE 802.11n communication performance in the presence of this type of jamming signals is presented in [5]. The aforementioned work carried out different measurements of achieved bit rate of an IEEE 802.11n communication in the presence of jamming signals considering the *sweep period* (SP) and *Interference Signal Ratio* (ISR) as test parameters.

Figure 3 presents bit rate measurements for 7 jamming signals with different SPs (20 μs, 10 μs, 6.4 μs, 5.5 μs, 1.6 μs, 1.06 μs and 0.64 μs). For each applied jamming signal, the achieved bit rate is given as a function of the ISR. A varying impact of the ISR on the communication performance is observed.

For instance, for an ISR lower than -26 dB and whatever the SP value, the achieved bit rate is maximum (95 Mbps), which means the system performance is not affected. However, for an ISR of -20 dB (6 dB stronger interference signal), there are different behaviors according to SP of the jamming signal. For an SP of 20 μs, the achieved bit rate is

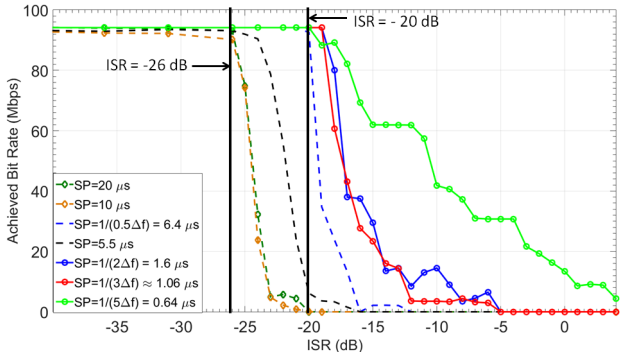

Figure 3. Bit Rate measurements of an IEEE 802.11n network, as a function of the ISR and different SP values.

0 bps (no communication) and for an SP of 0.64 μs it can reach the maximum rate. Indeed, the bit rate is affected and this depends on the SP of the interference signal.

To better understand these results, Figure 4 shows the required ISR levels to interrupt the communication, as a function of SP of jamming signal.

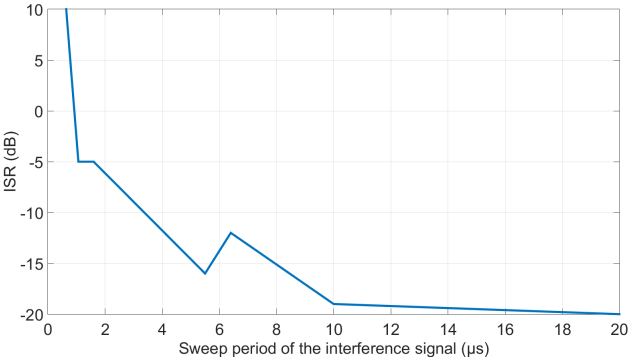

Figure 4. Required value of the ISR to completely interrupt the communication, as a function of the SP.

As shown in Figure 4, there is 30 dB difference between the required ISR for an SP of 0.64 μs and an SP of 20 μs. For SPs of 20 μs and 10 μs, the communication is interrupted with a jamming power level 20 dB below the communication. Nevertheless, the jamming signals with lower SP require more jamming power to degrade the communication. This is due to the transformation of the interference signal at OFDM receiver level.

Figure 5 displays the spectra of jamming signals obtained by FFT on 32768-point which corresponds to the OFDM symbol duration (3.2 μs) [6], that gives a subcarrier spacing Δf ($\Delta f = \frac{1}{3.2\ \mu s}$ [6]). We then observe that for an SP of $\frac{1}{3\Delta f}$, only one subcarrier out of 3 can be struck by the jamming signal, whereas for an SP of $\frac{1}{5\Delta f}$, only one subcarrier out of 5 can be struck by the jamming. Thus, when the SP decreases, fewer OFDM subcarriers are struck and the jamming signal is less efficient .

Furthermore, we notice the adaptation of *Modulation Cod-*

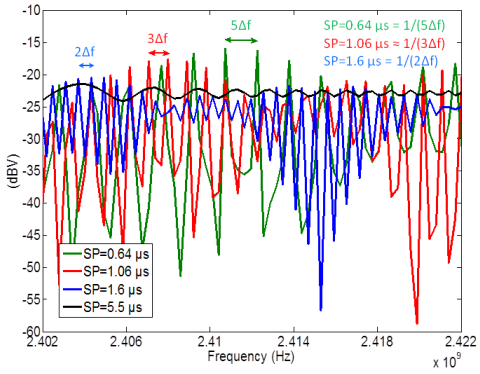

Figure 5. Spectra of the jamming signals obtained by FFT over a 3.2 μs window, for SP = 0.64, 1.06, 1.6 and 5.5 μs, between 2.402 GHz and 2.422 GHz.

ing Scheme mechanism for an SP of 0.64 μs. In this case, the MCS mechanism gradually reduces the bit rate to the conditions of the channel.

Finally, the jamming signal is less efficient when the SP is lower than 3.2 μs (OFDM symbol duration or time window W), due to its spectral distribution and the *Modulation Coding Scheme* mechanism.

4 Mitigation Technique

Based on the previous observations, in which the communication stayed robust facing a jamming signal with an SP of 0.64 μs that corresponds to one fifth the OFDM symbol duration ($\frac{3.2\ \mu s}{5} = \frac{W}{5}$), we propose to incorporate a simultaneous FFT module at OFDM receiver level with a window size wider than 3.2 μs (W).

Taking into account that the Wi-Fi communication presented greater vulnerability to the interference signal with SPs of 10 μs and 20 μs, the preliminary proposal consists in adding another FFT module in parallel with a window of 32 μs that corresponds to ten times the OFDM symbol duration ($10 \times W$) as presented in Figure 6.

Furthermore, since commercial jammers use an SP around 6 μs, the Wi-Fi communication is stronger facing these devices.

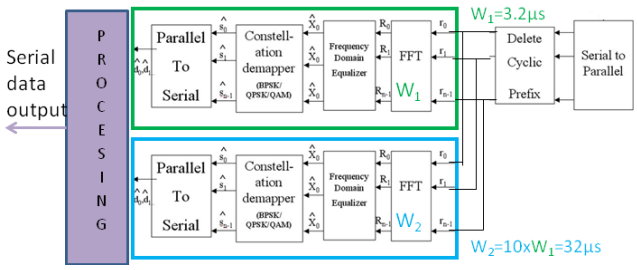

Figure 6. Proposed OFDM receiver system with two FFT windows in parallel.

5 Conclusion

This paper presents a study of jamming signals generated by low power commercial jammers. We studied the vulnerability of IEEE 802.11n communications to these signals, taking into account the sweep period (SP) and interference signal ratio (ISR) as test parameters. We identified the relationship between the SP and the FFT time windows used at receiver level. Indeed, for an SP inferior to 3.2 μs, the communication system can be considered robust. However, for SPs between 10 μs and 20 μs, the communication can be interrupted. We showed that the performance of IEEE 802.11n communications significantly depends on the SP. Therefore, we propose to incorporate another FFT module in parallel at OFDM receiver level, with a wider window than the current one, in order to reduce the IEEE 802.11n vulnerability facing jamming signals.

Acknowledgements

This work has been carried out in the framework of the ELSAT2020 project which is co-financed by the European Union with the European Regional Development Fund, the French state and the Hauts de France Region Council.

References

[1] G. Romero, E. Simon,, V. Deniau, C. Gransart and M. Kousri, "Evaluation of an IEEE 802.11 n Communication System in presence of Transient Electromagnetic Interferences from the Pantograph-Catenary Contact," *32nd URSI GASS*, Montreal, 19-26, August, 2017.

[2] W. Radasky, and e. Savage, "Intentional electromagnetic interference (IEMI) and its impact on the US power grid," *Meta*, pp.1-3, 2010.

[3] D. Giri, "High-power electromagnetic radiators: nonlethal weapons and other applications," *Harvard University Press*, 2004.

[4] R. Poisel, "Modern communications jamming principles and techniques," *Artech House*, 2011.

[5] V. Deniau, C. Gransart, G. Romero, E. Simon,and F. Joumana, " IEEE 802.11n Communications in the Presence of Frequency-Sweeping Interference Signals," *IEEE Transactions on Electromagnetic Compatibility*, **59**, 5, Oct, 2017.

[6] "IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Redline," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, 2012.