URSI AP-RASC 2019, New Delhi, India, 09 - 15 March 2019

Optimized Time-Frequency Processing Dedicated to the Detection of Jamming Attacks on Wi-Fi Communications

Mohamed Raouf Kousri [(1)], Virginie Deniau*[(1) (2)], Christophe Gransart [(1) (2)] and Jonathan Villain [(1)]
(1) Institute of Technological Research Railenium, Villeneuve dAscq 59650, France
(2) French Institute of Science and Technology for Transport, Development and Networks, Villeneuve dAscq 59650, France (e-mail: virginie.deniau@ifsttar.fr)

Abstract

Attacks by Jamming on wireless communication network can provoke Denial of Services. According to the communication system which is affected, the consequences can be more or less critical. In this paper, we propose to develop an algorithm which could be implemented at the reception stage of a communication terminal in order to detect the presence of jamming signals. The work is performed on Wi-Fi communication signals and demonstrates the necessity to have a specific signal processing at the reception stage to be able to detect the presence of jamming signals.

1. Introduction

Wireless communication systems can be vulnerable to Denial of Services attacks, provocked by jamming signals. Nowadays, while the use of jammers is prohibited, these devices are easily affordable on Internet and can affect a large number of communication systems. In the cases of wireless communication systems supporting security or operational functions, the consequences can be critical.
In this paper, the considered wireless communication technology is the Wi-Fi and more specifically the 802.11n, which is based on Orthogonal Frequency Division Multiplexing (OFDM) signals. Unlike other wireless technologies, Wi-Fi is vulnerable to low power levels of jamming which make these signals difficult to detect and observe [1]. This work presents a method able to extract and detect sweeping jamming signals even with high signal to jamming ratio (SJR).

Different jamming detection methods exist in the literature [2], but do not consider sweeping frequency jammers, which is the most frequent jamming technology. The method presented in this paper is based on an time-frequency analysis tool, which gives the possibility to adapt the analysis to both communication data and sweeping jamming signals.

After this introduction, the present paper first describes the main characteristics of considered jamming signals and the 802.11n protocol. Then, the whole experimental setup is detailed and we present and analyze the developed post processing to detect the presence of jamming signals. Finally, results are presented and discussed.

2. Impact of Jamming signals on Wi-Fi

In the literature, a large number of jamming signals are mentioned [3] [4]. However, in practice, the major part of the jammers found on the Internet are frequency sweeping jammers. These jammers emit signals over the frequency band employed by a communication system to corrupt the reception quality. Fig. 1 is a time-frequency representation of this type of jamming, and shows how the signal sweeps the Wi-Fi 2.4 GHz band every 10 µs.

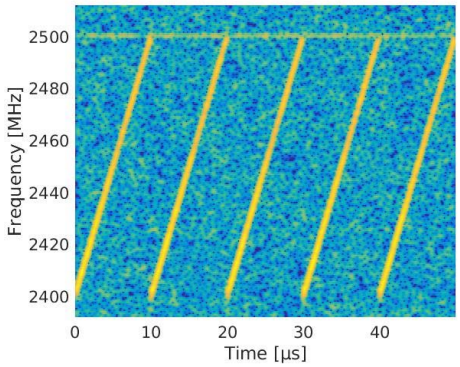

Figure 1. Time-frequency representation of a jamming signal.

The power level of jamming signal required to corrupt the communication can be different according to the communication system. To understand the action of the jamming signal, the Wi-Fi protocol is detailed.

2.1 Wi-Fi protocol

The 802.11n standard is based on the OFDM encoding method to send data over 20 MHz or 40 MHz channels. OFDM is a parallel transmission scheme, where a high rate serial data stream is split up into several sub streams, each of which being modulated on a separate subcarrier. The subcarrier spacing is denoted Δf. To obtain high spectral efficiency, adjacent subcarriers are modulated by selecting

orthogonal frequencies, i.e. $\Delta f = 1/T$, where T is the duration of the OFDM symbol.

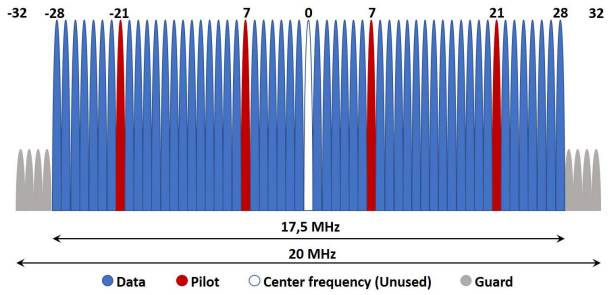

Figure 2. Subcarriers distribution in a 802.11n channel.

The 20 MHz channel includes 64 possible subcarriers, only 52 of them are used for data transfer, 4 are used as pilot symbols, and 8 are guard subcarriers [5]. These 8 guard subcarriers are empty, and are used to prevent interferences between adjacent Wi-Fi channels.

2.2 Jamming impact

Measurements were carried out in an anechoic chamber to assess the impact of a jamming signal on a 802.11 n communication, as showed in Fig. 3.

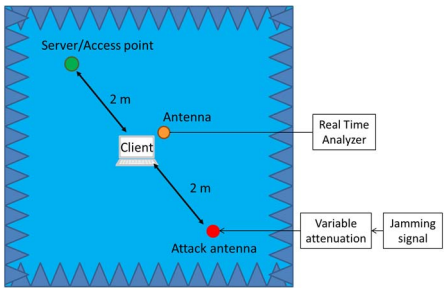

Figure 3. Measurement configuration.

An omnidirectional antenna (EM-6116) was connected to a real time analyzer and placed at the proximity of the client computer in order to assess the received power similarly to it. The jamming signal was strongly attenuated using an attenuation control unit and we reduced step by step the attenuation up to the whole loss of the communication. For each attenuation value, the bit rate was measured, by means of Iperf3 program [6] which was running on the client side.

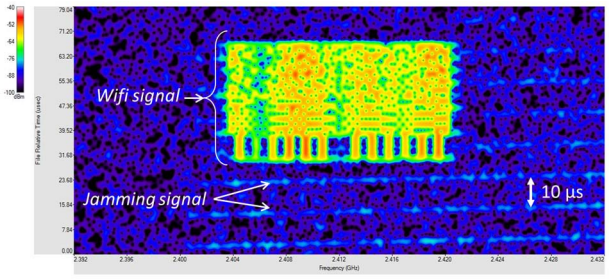

Figure 4. Time - Frequency representation of a wifi communication signals in presence of jamming.

The measurement result presented Fig. 4 corresponds to the case where the jamming signal power is 1 dB inferior to the level required to loose the communication, i.e. the bit rate reached zero. The jamming signal power is significantly lower than the Wi-Fi communication signal. Indeed, Wi-Fi is strongly vulnerable to the presence of jamming signals due to the Clear Channel Assessment-Energy Detect (CCA-ED) mechanism applied to sense the medium at the PHY layer [1]. According to [7], CCA-ED consists in measuring the highest average power over the channel. The CCA-ED indicates a channel as busy when the received signal strength exceeds -72 dBm (for 20 MHz bandwidth) [7, p. 1614]. The jamming then affects the power measured by the CCA-ED algorithm, which judges the channel as busy and the client is not able to access the medium.
Such a low power level of jamming signals, but high enough to interrupt the communication, needs a dedicated process for detection.

3. Detection principle

The shape of any measured signal depends on the measuring system parameters. When a signal is measured in the time domain, the time-frequency processing and the processing parameters significantly impact the obtained time-frequency distribution. In the case of Wi-Fi, the reception stage collects the signal in the time domain and applies an FFT to obtain the time-frequency distribution. The sampling and the FFT time windows are defined to obtain a frequency resolution corresponding to a 312.5 kHz spacing between subcarriers. The jamming detection that we suggest consists in applying at the reception a specific time-frequency processing which improves the reception of the jamming signal and makes it easier to detect.

3.1 Wi-Fi signal processing

In order to demonstrate the importance of adapting the processing for detection, we performed a processing similar to those carried out by a Wi-Fi receiver. Wi-Fi and jamming signals were measured using real time spectrum analyzer. A FFT was applied using a 3.2 µs rectangular time window. Fig. 5 presents the results of this analysis by showing the power measured along the time for the different subcarriers of an acknowledgement (ACK) frame.

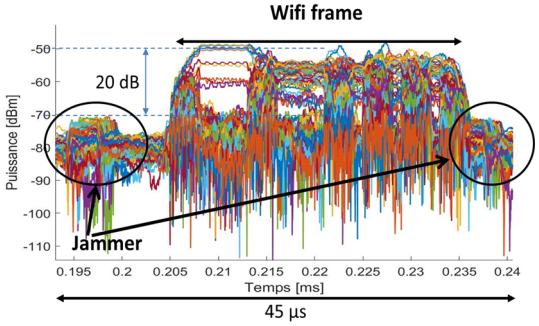

Figure 5. Power of the different sub-carriers along the time.

We can see on Fig. 5, an ACK frame, with the preamble in

its beginning, followed by 4 OFDM symbols. We also observe before and after this frame, the appearance of the jamming signal. It is only visible in the absence of Wi-Fi transmitted data, and almost invisible during the ACK frame, while it occurs each 10 µs. We observe that its power level is 20 dB less than Wi-Fi signals, despite the fact that at this jamming level, Wi-Fi communication is about to be interrupted.

3.1 Jamming detection processing

The first idea of the proposed method is to concentrate the analysis on the first and the last guard frequencies of the Wi-Fi channel. These frequencies are unoccupied by the Wi-Fi, that should facilitate the detection of jamming signals. In the first step, a discrete Fourier Transform (DFT) is applied to the measured signal. This DFT is only performed on the first and the last guard frequencies, Fg_1 and Fg_2 as shown in Eq. 1.

$$X_{1DFT} = x * \exp(-j2\pi F_{g1}.t) \qquad (1).$$

As seen in the previous paragraph, jamming signals are difficult to observe using a 3.2 µs analysis window. Generally speaking, the width of the analysis window must be in the same range of any analyzed phenomena in order to avoid to spread its power over a wide time window. The analysis window must be adapted to the characteristics of jamming signals over the Wi-Fi channel. In Fig. 5, whereas the jamming signal is continuous in time, it occurs instantly on each subcarrier at a time. In the same figure, the duration and the power level of this phenomena is related to the width of the analysis window. Using a shorter window, the occurrence of the jamming signal on each sub-carrier will appear shorter in time and more powerful. Nevertheless, short analysis windows induce poor frequency resolutions. A compromise must be taken in the choice of the analysis window width. In the one hand, it should allow us to obtain a high enough jamming signal power level. On the other hand, a good frequency resolution is required to avoid any influence from the used sub-carriers on the first and the last guard frequencies [7].
We then use a time-frequency process optimizing the time and frequency resolutions, using a rectangular time window. The width of this window determines the time and the frequency resolutions, and it is chosen regarding the frequency gap between the last used sub-carrier and the guard frequencies, which corresponds to 1.25 MHz. As a consequence, the width of the adequate rectangular window is equal to 0.8 µs (1/1.25 MHz = 0.8 µs). In the frequency domain, the spectrum of this window is null at the last used subcarrier. Moreover, to reduce the impact of the side lobs of the rectangular window, the process applies a multi convolution technique detailed in [8].

This processing is performed on sampled signals, thus the 0.8 µs window corresponds to a number of samples which depends on the sampling frequency. Since the window is rectangular, the convolution is reduced to a simple sum of the samples over its width as outlined in Eq.2.

$$X(i)_{DFT} = \frac{\sum_{n=i}^{w+i} x(n)_{DFT}}{w} \qquad (2).$$

Where w represents the width of the analysis window, and $x(n)_{DFT}$ is the result of Eq. 1.
This process is performed throughout the entire signal. But the use of a rectangular time window permits us to obtain a maximum time resolution by shifting the windows of a single sample per step, without very time-consuming calculations. To obtain the next value $X(i+1)_{DFT}$, the computation of the sum over the full width w is not necessary. We subtract the first sample $x(i)_{DFT}$ and add the following sample $x(i+w+1)_{DFT}$.
By performing this processing 3 successive times, corresponding to the 3 convolutions, we reduce the impact of the side lobs of the rectangular window by 26 dB and maintain a frequency resolution of 1.25 MHz.
Fig. 7 compares the power observed over 0.1 ms on the first guard sub-carrier by two different processes. Fig. 7.(a). is the result of the proposed method using a 0.8 µs rectangular window and 3 successive convolutions. Fig. 7.(b), is the result by applying a receiving process similar to the Wi-Fi terminal, which means an FFT over a 3.2 µs rectangular window. The occurrence of the jamming signal is clearly highlighted in Fig. 7.(a). The short duration of the analysis window increases the calculated power of the jamming signal which appears more powerful than the rest of the signal. On the other hand, the 3 successive convolutions limit the impact of the Wi-Fi data signals on the guard frequency by reducing the analysis window side lobs. In Fig. 7.(b), the jamming signal is no more discernible.

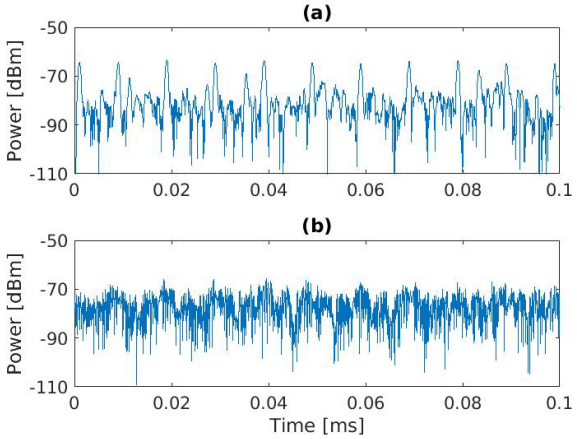

Figure 7. Shape of the guard frequency with different processes (a). w = 0.8 µs and 3 convolutions: Proposed method. (b). w = 3.2 µs and 1 convolution: Wi-Fi processing method.

4. Detection

This work illustrates the relevance of performing an optimized processing which gives the ability to distinguish the presence of low power jamming signal superimposed to Wi-Fi communications. Once the jamming signal is

made visible by the processing, the detection may be more effective. An example of a detection method that could be used is autocorrelation. Indeed, Fig. 7.(a) shows that the jamming signal occurs regularly on the guard subcarriers. The time gap between each occurrence is the jammer sweep time, here 10 µs. This regularity can be detected by autocorrelation. Applying this function on a repetitive signal gives a typical pattern that matches the jamming signal occurrence on the guard sub-carrier. Fig. 8 gives the result of the autocorrelation performed on the signal presented in Fig.7.(a) and on another Wi-Fi signal without jamming.

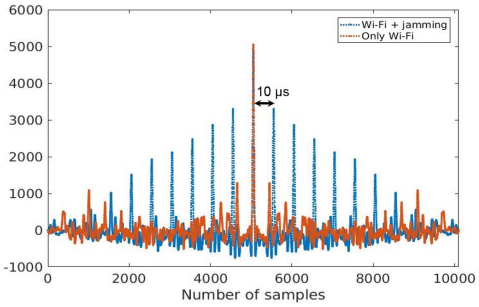

Figure 7. Results of the autocorrelation of pre-analyzed sub-carrier signals with and without jamming signals.

The blue curve, for the jammed signal, has a recognizable pattern that indicates the presence of a jamming signal and its sweep time, which corresponds to the spacing between the spikes of the curve. The orange auto-correlation curve corresponding to Wi-Fi signal without jamming, has a random shape that does not contain any pattern. The clear difference between both patterns can permit to implement an automatic detection process.

5. Conclusion

This paper presents an adapted processing which aims to highlight the presence of a low power jamming signal superimposed to an IEEE 802.11n communication. The time-frequency algorithm is based on a DFT using a rectangular window adapted to the characteristics of both jamming and IEEE 802.11n signals. The DFT is performed on the guard sub-carriers of the Wi-Fi channel, and the analysis, using a 3 successive convolution process with the rectangular window, allows us to increase the power of the jamming signals, while reducing the impact of the Wi-Fi data signals on the guard sub-carriers. Hence, we obtain a shape significantly impacted by the jamming and which allows its efficient detection. This paper also illustrates that a detection based on the autocorrelation could be easy to implement even if the signal is correctly processed at the receiving stage. Since the jamming signal occurs with a regular rate, performing an autocorrelation on the analyzed signal permits to observe a typical pattern of the jamming signal presence. Moreover, at the difference of other detection methods based on Error Vector Magnitude (EVM) or the state of the data frames [2], the proposed approach does not require demodulation, which facilitates its implementation on a Software Defined Radio (SDR) device.

6. Acknowledgements

This work was performed in the framework of the X2Rail1 project (Shift2Rail Joint Undertaking) and 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.

7. References

1. V. Deniau; C. Gransart; Grecia L. Romero; E. P. Simon; J. Farah, IEEE 802.11n Communications in the Presence of Frequency-Sweeping Interference Signals, IEEE Transactions on EMC, vol. 59, no. 5, pp. 1625-1633, 2017.

2. R. Bhojani, R. Joshi, An Integrated Approach for Jammer Detection using Software Defined Radio, Procedia Computer Science, vol. 79, pp. 809-816, 2016.

3. R. Poisel, Modern Communications Jamming: Principles and Techniques. Artech House. ISBN: 9781608071654, 2011.

4. K. Pelechrinis, M. Iliofotou & S. V. Krishnamurthy, V. Denial of Service Attacks in Wireless Networks: The Case of Jammers, IEEE Communications Surveys Tutorials, 16, 13, pp.245-257, 2011.

6. IEEE Std 802.11-2012, 2012. 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.

7. iPerf, The ultimate speed test tool for TCP, UDP and SCTP, https://iperf.fr

8. G. Betta, D. Capriglione, G. Miele and L. Rossi, Reliable Measurements of Wi-Fi Electromagnetic Pollution by Means of Traditional Spectrum Analyzers, 2008 IEEE Instrumentation and Measurement Technology Conference, Victoria, BC, pp. 206-211, 2008.

9. M.R. Kousri, V. Deniau, M. Heddebaut, S. Baranowski, J. Rioult, Time- frequency processing adapted for the different electromagnetic compatibility issues in the railway domain, IEEE International Symposium on EMC, Dresden, pp. 1272-1277, 2015.