PROCEEDINGS OF SCIENCE

Strategy for WiFi interference detection in weather radar applications

Andy Moreno Rodríguez,[a,b] **Jorge Cogo**[c,*] **and Juan Pablo Pascual**[a,b]

[a] *Instituto Balseiro, Universidad Nacional de Cuyo - Comisión Nacional de Energía Atómica (CNEA), Av. Bustillo 9500, San Carlos de Bariloche, Río Negro, Argentina*

[b] *Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)*

[c] *Universidad Nacional de Río Negro, Anasagasti 1463, San Carlos de Bariloche, Río Negro, Argentina*

E-mail: andy.moreno@ib.edu.ar, jcogo@unrn.edu.ar, juanpablo.pascual@ib.edu.ar

The interference due to WiFi devices degrades the quality of the products obtained by C-band weather radars. In this work we present a strategy for detecting these interfering WiFi packets in the radar output signal. The method is based on a delay and correlate algorithm, which takes advantage of the periodic structure of the WiFi packets preamble, periodicity that is preserved even when the signal is distorted when passing through the radar reception stages. We formulate the detection strategy as an hypothesis test that uses the squared modulus of the auto-correlation as the statistic. With this formulation we obtain the decision threshold as a function of the desired false alarm probability. We perform a series of controlled experiments using real weather radar data collected by Argentinian C-band RMA radars. The results show a high detection rate both when the WiFi interference is in regions where there is only additive noise and when it is in regions where there is also a meteorological target.

RFI 2024 Conference
14-18 October 2024
Bariloche, Argentina

*Speaker

PoS(RFI2024)034

1. Introduction

In 2003 the International Telecommunication Union (ITU) decided to assign the frequency bands 5.150-5.350 and 5.470-5.725 GHz to wireless access systems, including Wireless/Radio Local Area Networks (WLAN/RLAN), as long as they do not cause interference to existing systems that operate in these bands, such as C-band weather radars. The idea was that they coexist with weather radars, requiring wireless access systems use a dynamic frequency selection function (DFS) to check for the presence of radar signals before transmitting on a given channel. However, even today interference caused by wireless networks devices to C-band weather radars is one of the limiting factors of their performance [1]. In general, the wireless networks devices in operation today are based on the IEEE 802.11 standards and are referred to as WiFi.

Figure 1(a) shows the reflectivity plan position indicator (PPI) of the measurements collected by the RMA1 Argentinean C-band weather radar, located in Córdoba city. The image corresponds to a complete sweep of the horizontal polarization (HH), at 0.5 degrees of elevation, taken under clear air conditions. The lines oriented radially toward the radar position correspond to WiFi interference.

A challenge of the signal processing stage consists in identify the WiFi interference in order to reduce its effect over the weather radar products. There are techniques that identify the WiFi signals based on polarization properties [2] and by image processing methods [3]. It is also possible detect the interference using the deterministic waveform of the WiFi preamble at the correlation stage output [4]. In this work, we tackle the problem of of detecting the WiFi interference in the weather radar from the periodic components of its signal structure.

2. Problem formulation

The IEEE standards 802.11a,ac,ax describe the physical layer specifications for WiFi systems that use orthogonal frequency division multiplexing (OFDM) in the 5 GHz band. The data packets of the different clauses contain a preamble compatible with standard 802.11a operating in a 20 MHz channel bandwidth in the 5 GHz band. This preamble consists of a sequence of ten short symbols followed by a sequence of two long symbols. Each short symbol has a duration of 0.8 μs which results in a periodicity of this time interval. The long symbols have a length of 3.2 μs with a cyclic prefix of 1.6 μs, which gives a total preamble duration of 16 μs. Even when the C band weather radar systems operate in the same carrier frequencies range, the WiFi signal is completely distorted by the radar front-end and matched filter, mainly because the system bandwidth and sampling frequency are different to the required for the interfering signal. However, the periodic structures of the preamble remain after matched filter output. This can be observed in Figure 1 (b), where it is showed the in-phase component of a WiFi packet at RMA1 matched filter output. The plot corresponds to the received signal for one particular pulse of the dataset described in the previous section, where there are only two WiFi signal packets plus noise.

In digital communication systems, periodic structures of the training sequences are used to symbol detection, timing and measuring the carrier frequency offset [5]. One simple method is the delay and correlate algorithm, which searches for repetition in the received signal using a correlator and a maximum finder. Let $y[m]$ be the received discrete-time baseband signal, then the

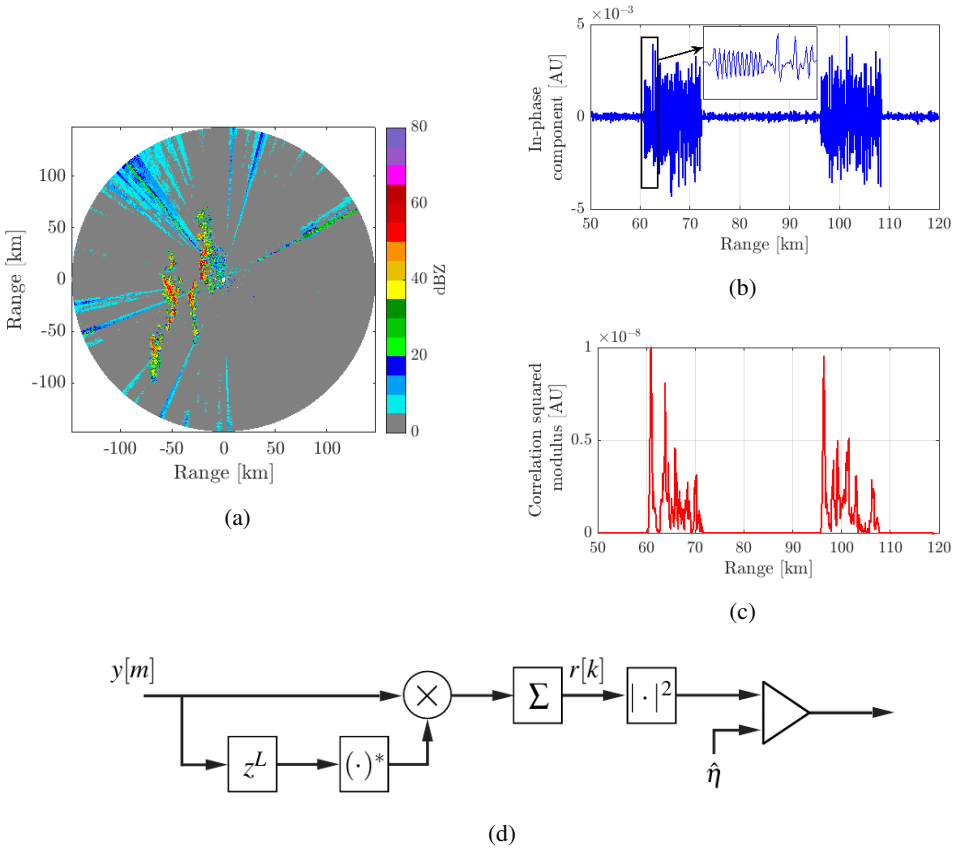

Figure 1: (a) PPI of reflectivity. (b) WiFi signal in weather data recorded. (c) Squared modulus of the weather data recorded auto-correlation. (d) Block diagram of the detection algorithm.

auto-correlation, $r[k]$, of the received signal is given by

$$r[k] = \sum_{m=0}^{M-1} y^*[m+k]\,y[m+k+L], \tag{1}$$

where M is the repetition interval length and L is the separation between two adjacent intervals.

3. Interference detection algorithm

We propose an algorithm that takes advantage of the preamble periodic structures including in the OFDM frames to detect WiFi packets in the weather radar data. The detection strategy consists in an hypothesis test that employs the squared modulus of the auto-correlation $r[k]$, i.e. $|r[k]|^2$ as the decision statistic, which is compared with a threshold, $\hat{\eta}$. The derivation of the test allows to determine the threshold value, $\hat{\eta}$. We use the sequence of five short symbols, which is repeated twice, as the periodic structure. Then, we set $M = L$ and equal to the number of samples of five short symbols. Figure 1(c) shows $|r[k]|^2$, where a peak is observed at the beginning of each packet. Figure 1(d) shows the block diagram of the detection algorithm proposed.

The detection procedure is given by the decision between the two hypotheses $H_0 : y[m] = w[m]$ and $H_1 : y[m] = x[m - m_i] + w[m]$, after $y[m]$ has been received from the range cell under test,

being $w[m] \sim \mathcal{CN}(0, \sigma^2)$, and $x[m]$ represents the WiFi signal preamble, which starts with the ten short symbols. We define $s[m]$ as the waveform of five consecutive short symbols.

At the decision instant the auto-correlation output is given by

$$H_0 : r[m_i] = W_0 \tag{2}$$

$$H_1 : r[m_i] = E_s + W_1, \tag{3}$$

where $E_s = \sum_{m=0}^{L-1} |s[m]|^2$. Based on the central limit theorem (CLT) the noise components can be modeled as $W_0 \sim \mathcal{CN}(0, L\sigma^4)$ and $W_1 \sim \mathcal{CN}(0, 2E_s\sigma^2 + L\sigma^4)$. Assuming that σ^2 is known, the decision threshold results $\eta = -L\sigma^4 \ln(P_{FA})$, where P_{FA} is the false alarm probability of the test. In practice the noise power, σ^2, is unknown and should be estimated. A solution consists in extend the formulation to a constant false alarm rate (CFAR) test [6], which leads to the threshold

$$\hat{\eta} = (P_{FA}^{1/N} - 1) \sum_{n=1}^{N} z_n, \tag{4}$$

where z_n represents independent samples of $|W_0|^2$

4. Results

In order to evaluate the performance of the presented detector, we performed a series of controlled experiments using real weather radar data. In-phase (I) and quadrature (Q) samples of WiFi packets were extracted from the RMA1 radar dataset described in Section 1 and they were added to the I and Q samples acquired by the weather radar RMA6, located in Mar del Plata city, under rainy conditions, where there was no evidence of WiFi interference. The carrier frequency, sampling rate and polarization of both datasets are the same. Then, the detection algorithm was run on the combined dataset. Based on the WiFi preamble length and the data sampling rate, $L = M = 20$ was set and $N = 11$ of z_n samples were considered. The samples I and Q that were classified belong to hypothesis H_1 were set to zero. The reflectivity PPI was calculated with the combined and with the output datasets. Two situations were considered. First, the WiFi samples were added in a region where only noise was present. The reflectivity before and after applying the detection algorithm are presented in Figures 2(a) and 2(b), respectively. In this case, the detection rate was 100%, due to the high ratio of interference power to noise power. Second, the WiFi samples were added in a region where a meteorological target was also present. The reflectivity before and after detection are presented in Figures 2(c) and 2(d). In this case, the detection rate was 98%.

5. Conclusions

We proposed a strategy for the detection of WiFi signals that interfere C-band weather radars. It operates over the signal received by the radar and uses the periodic structure of the preamble of the OFDM-based WiFi signals. The squared modulus of the radar signal auto-correlation was used as decision statistic. The threshold was obtained by means of an hypothesis test formulation, considering a CFAR approach. Finally, the performance of the algorithm was validated using measurements of Argentinean C-band radars, showing a high detection rate. As future step, it is necessary to design a method to define the WiFi packet length to be removed once it is identified.

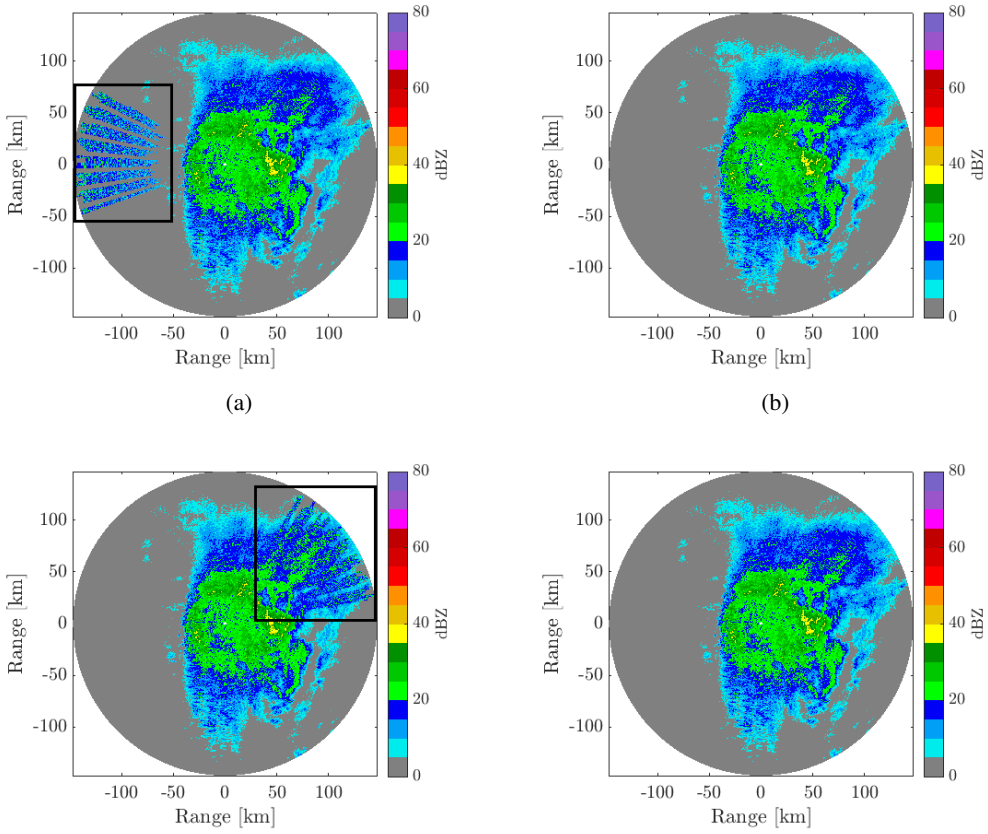

Figure 2: Reflectivity of the combined dataset. (a) Input of the first experiment. (b) Output of the first experiment. (c) Input of the second experiment. (d) Output of the second experiment.

References

[1] E. Saltikoff, J. Cho, P. Tristant, A. Huuskonen, L. Allmon, R. Cook et al., *The threat to weather radars by wireless technology*, *Bull. Amer. Meteor. Soc.* **97** (2016) 1159.

[2] R. Keränen, H.F. V. Oyj, L. Rojas and P. Nyberg, *Progress in mitigation of WLAN interference at weather radar*, in *36th Radar Meteorol.*, (Colorado, VA), pp. P15.336 1–8, 2013.

[3] M. Peura, *Computer vision methods for anomaly removal*, in *2nd Eur. Conf. Radar Meteorol. Hydrol. (ERAD)*, (Delft, Netherlands), pp. 312–317, 2002.

[4] O. Barba Leal, F. Rinalde, J. Cogo and J. Pascual, *WLAN signal detection in weather radar data*, in *XIX Workshop Inf. Process. and Control (RPIC'21)*, (San Juan, Argentina), 2021.

[5] M. Morelli and U. Mengali, *Carrier-frequency estimation for transmissions over selective channels*, *IEEE Trans. Commun.* **48** (2000) 1580–1589.

[6] M.A. Richards, *Fundamentals of Radar Signal Processing*, McGraw-Hill, New York (2005).