Monitoring building radio frequency activity in order to locate the jamming source position by classification

Villain Jonathan, Mickael Dufour, Nicolas Thouvenin, Paul Monferran, Virginie Deniau, Christophe Gransart

Monitoring building radio frequency activity in order to locate the jamming source position by classification.

Jonathan Villain, Mickael Dufour, Nicolas Thouvenin, Paul Monferran, Virginie Deniau, Christophe Gransart
COSYS-LEOST, Université Gustave Eiffel, 20 Rue Élisée Reclus, 59650 Villeneuve-d'Ascq, France
CERI SN, IMT Nord Europe, Rue Guglielmo Marconi, 59650 Villeneuve-d'Ascq, France
Inodesign, 155 Avenue Georges Hannart, 59170 CROIX, France
jonathan.villain@imt-nord-europe.fr

***Abstract*—In this work, we evaluated the performances of different Machine Learning algorithm to locate the source of a jamming signal in a building. The results presented here are part of a wider project dealing with the monitoring of wireless communication system. Jamming signal are difficult to manage. To help manage these attacks, we deployed a monitoring system permitting to locate the source of the jamming signal.**

***Index Terms*—RF signal, detection system, location system, machine learning, wireless communication.**

I. Introduction

Discussions of Intentional Electromagnetic Interferences were once largely confined to electronic warfare forums. The risks of poor protection of a wireless network are various. It is possible to interact with the communications whether to scramble video surveillance, to interrupt calls, to retrieve personal information or to induce themselves into a secure system. However, behind the Intentional Interference, we can mention the jamming interference which is a kind of interference specifically designed to affect the communications between the public electronic or communication components. Consequently, with the rise of wireless communications in infrastructures jamming has become a mainstream topic. Many studies work on the location of the signal source [1]–[3]. But most of these studies are in an outdoor context, in simulation or use data from higher layer than the physical layer. Some of our previous work focus on the detection of jamming signal [4] and estimating the distance of the signal [5].

In this study, the section II describes an experimentation permitting to locate in which area of a building is the source of a jamming signal. The section III discusses about the deployed Machine Learning algorithm to identify in which area of the building is the jammer.

II. Scenario

This study aims to detect the source of a jamming signal in an indoor public area. The following will describe the Equipment, the measurement environment and the protocol of the attack studied.

A. Equipment

For the study, the monitoring system deployed is composed of :

- Two SDR (System Define Radio) developped by Inodesign,
- Eigh omnidirectional antenna,
- Eigh 20 cm SMA M/F transition cables, 4 meters long,
- Two support 4 antennas (see Figure 1).

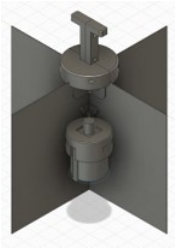

Fig. 1. Representations of antennas.

We also used a commercial jammer which covers the frequencies from 2.5 GHz to 2.7 GHz.

B. Measurement environment

To test our approach we deployed a monitoring system in a building of Gustave Eiffel University. The building is divided into 11 areas (CEM, ESTAS, LEOST, Railenium, Repro, Etage, Outdoor, Hall, Coffee, Europe and Flandre). In this experimentation, we choose to collocate four antennas in each side of the building. The Figure 2 shows the arrangement of equipment in the building. These antennas are separated by a deflector attached to the support (see Figure 1). The SDR permits to synchronize the acquisition on four antennas. The two SDR are synchronized one with another using the internal computer clock. With this system, we monitor 245.76 MHz of band centered on 2.6 GHz. The sampling rate is 245.76 MHz for a time window of 0.133 ms. The source of the jamming signal used is a commercial jammer which covers the band studied.

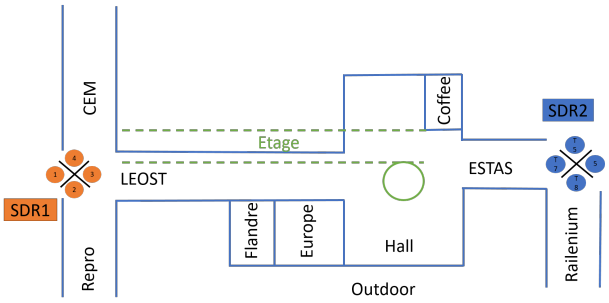

Fig. 2. Experimentation carried out in Gustave Eiffel University.

C. Attack

We want to determine in which area is located the source of the jamming signal. For this purpose, a person carrying a commercial jammer moves during 5 minutes in one of the areas of the building. We repeat this measurement for each area. With this experimentation, we collected, for one antenna, 300 measurements per area.

III. Discussion

In this section, we will discuss about the jammer location. We will start by explaining the choice behind the input of our learning process and compare some Machine Learning algorithm used to locate the source of the jamming signal.

A. Data

During the experimentation, the two SDR allowed us to collect 3300 measurements of the electromagnetic activity. Each measurement is composed of eigh IQ data sheets organised in a matrix 32768×2. After analysing the jamming signal (see Figure3), to reduce the calculation time, we choose to use 3000 samples to calculate the FFT which correspond to two periods of the jamming signal. In the following, we will use the data from the FFT to feed our location algorithms.

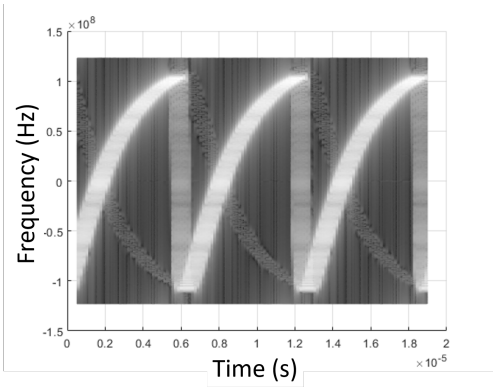

Fig. 3. Spectrogram based on Short Fourier Transform of the jamming signal.

B. Location

For the location, the collected data are organised in a training and testing set containing respectively 80% and 20% of the data. The tested algorithms are Random Forest (RF), Linear Discriminant Analysis (LDA), linear Support Vector Machine (LSVM), Kernel Support Vector Machine classification (SVMc) and K nearest neighbour (KNN). For the learning process, the models is estimated by a five-fold cross-validation process on the training set. The criterion used to compare the different models is the error of classification in percent. For each algorithm we estimate two models. One is estimated from the input data calculate by the FFT on 3000 sample (FFT). A second is estimated from the mean of the FFT (MFFT). The errors are presented in table I.

TABLE I
Classification error of the models on the test set

	classification error in %	
models	FFT	MFFT
LDA	10,6	26,3
LSVC	8.5	68.2
SVMc	58,6	16.1
RF	22,1	16.7
KNN	13.2	16.1

If we consider the FFT on 3000 sample as an input, the best models are the linear one and KNN. In fact, the SVMc is excessively flexible on the edges of the learning domain to perform well on these data. For RF, the correlation of the different feature makes it difficult to generate trees. Using the mean value of the FFT permits to improve the quality of these two models but has the opposite effect on the linear one. The more robust which can be consider as not impacted by the change in the feature is KNN and it produces good results to predict the area where is the jammer.

IV. Conclusion

In this study we propose a monitoring system permitting to localise in which area is a commercial jammer. To monitor a building we focus on estimating in which area is the source of the jamming signal. To do so we focused our approach on the physical layer using the result of the FFT of the signal. Linear models perform well in predicting the area where the jammer is but KNN seems more robust in its prediction. In future work we will study other configurations to monitor the building.

References

[1] Liu, H., Liu, Z., Chen, Y., Xu, W. (2011). Determining the position of a jammer using a virtual-force iterative approach. Wireless Networks, 17, 531-547.

[2] Yang, F., Shu, N., Hu, C., Huang, J., Niu, Z. (2023). Jammer Location-Aware Method in Wireless Sensor Networks Based on Fibonacci Branch Search. Journal of Sensors, 2023.

[3] Olsson, G. K., Nilsson, S., Axell, E., Larsson, E. G., Papadimitratos, P. (2023, April). Using Mobile Phones for Participatory Detection and Localization of a GNSS Jammer. In 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS) (pp. 536-541). IEEE.

[4] Villain, J., Deniau, V., Gransart, C., Fleury, A., Simon, E. P. (2021). Characterization of IEEE 802.11 communications and detection of low-power jamming attacks in noncontrolled environment based on a clustering study. IEEE Systems Journal, 16(1), 683-692.

[5] Villain, J., Deniau, V., Gransart, C. (2022). Jamming Detection in Electromagnetic Communication with Machine Learning: A Survey and Perspective. In Machine Learning and Probabilistic Graphical Models for Decision Support Systems (pp. 252-271). CRC Press.