Characterization of IEEE 802.11 communications and detection of low power jamming attacks in noncontrolled environment based on a clustering study

Jonathan Villain, Virginie Deniau, Christophe Gransart, Anthony Fleury, Eric Pierre Simon

Characterization of IEEE 802.11 communications and detection of low power jamming attacks in non controlled environment based on a clustering study

Jonathan Villain[1], Virginie Deniau[1], Christophe Gransart[1], Anthony Fleury[2], *Member, IEEE*, and Eric Pierre Simon[3]

***Abstract*—Wireless connections are more and more used in different applications and in public areas for services to consumers but also for handling (sometimes) sensitive communications (for instance in railway systems or for remote video monitoring systems). Such systems can have to face different kind of attacks that target the behind service. Our work aims to detect, as soon as possible and online, attacks that can occur on wireless networks, to be able to react very quickly. In this paper, we present some results of data analysis methods, on Wi-Fi signals, to differentiate the ones with attacks from the ones without. This study focuses on low power jamming attacks with a slight or even no impact on Wi-Fi communications. This is more challenging than detecting high power jamming attacks which have already been addressed in the literature. Being able to detect a low impact attack is a crucial issue in a global security strategy, making it possible to launch countermeasures before the interruption of the communication. The Wi-Fi bands are also in the ISM frequencies, making the environment complicated to analyze. Clustering methods such as Agglomerative Hierarchical Clustering are used to identify some clusters and then to map them to the real classes (with or without attacks). A deep analysis of the clusters obtained in a dataset acquired in uncontrolled conditions is carried out. This is done in order to understand what is responsible of the clustering assignment of the different points and to extract the clusters which can be used to design a detection attack strategy.**

***Index Terms*—IEMI, Intentional ElectroMagnetic Interference, Classification, Wlan, Wi-Fi, communication network journal, IEEE 802.11n.**

I. Nomenclature

AWG	Arbitrary Waveform Generator
AHC	Agglomerative Hierarchical Classification
IDS	Intrusion Detection System
ISM	Industrial, Scientific and Medical
PCA	Principal Component Analysis
SVM	Support Vector Machine
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
Wi-Fi	Wireless Fidelity

Manuscript received December 22, 2020.

* Designates the corresponding author: Jonathan Villain, PhD, University Gustave Eiffel, jonathan.villain@univ-eiffel.fr

[1] University Gustave Eiffel, IFSTTAR, COSYS-LEOST F-59650 Villeneuve d'Ascq, France . e-mails: virginie.deniau@univ-eiffel.fr christophe.gransart@univ-eiffel.fr

[2] IMT Lille Douai, Institut Mines-Télécom, Univ. Lille, Center for Digital Systems, F-59000 Lille, France. e-mail: anthony.fleury@imt-lille-douai.fr

[3] IEMN lab, TELICE group, University of Lille, France. e-mail: eric.simon@univ-lille.fr

II. Introduction

THE ISM bands are frequency bands that can be used for industrial, scientific, medical, domestic and short-range applications. ISM bands include the 2.4 GHz-2.5 GHz frequency band in which Wi-Fi networks and Bluetooth communications operate, as well as many public and consumer wireless applications. These include professional and domestic video surveillance cameras, webcams, door remote controls and, more generally, many home automation equipment.

A. Motivation

In the industrial field, with the increasing use of tablets or smartphones (including devices not owned by the companies – "Bring your own device" being a policy that has quickly spread), more and more operational functions are operated by wireless solutions using this ISM band. However, these communications can be very vulnerable to intentional electromagnetic interferences, making it easy for malicious individuals to carry out denial of service attacks. This is due to two facts:

- the ISM communication signals are relatively low power signals due to the fact that the permitted transmit powers in the ISM bands are limited by standards.
- the radio communication jammers generally cover this 2.4 GHz-2.5 GHz frequency band with a sufficient power level to disturb the communication signal.

Although the use of communication jammers is prohibited, they are generally employed for malicious actions. They can be used by hackers to jam the video transmission of surveillance equipment. Facing these risks, it becomes necessary to detect the presence of communication jammers in order to protect critical functions [1] managed by communication protocols operating in this ISM band. The purpose of this article is therefore to detect jamming attacks on a Wi-Fi network by monitoring the physical layer. The interest of working on the physical link is that we avoid problems related to privacy issues. Besides, jamming attacks are difficult to differentiate from other forms of interference by observing the upper layers. This approach to the surveillance of the physical link is also studied in the field of connected vehicles [2]. The data we recover corresponds to the electromagnetic activity, i.e. spectra collected from antennas integrated in the monitored environment. It is therefore a very different approach from IDS that monitor data located on higher layers. One of the

difficulties of the subject is that we must be able to detect interferences whatever the ambient electromagnetic activity, activity over which we have no control and no model. Indeed within the same place, the activity, on a monitored Wi-Fi band, can be very variable according to the hours of the day. In fact, today, for example, anyone can create an access point using their smartphone and thus modify the network. To adapt to this variability of the environment, unsupervised machine learning approaches are particularly appropriate [3] [4]. One of the difficulties, in an open environment, will be to detect low-power jamming attacks.

The detection approach studied in this article aims to characterize very weak jamming signals with very little impact or even no impact on Wi-Fi communication. This is more challenging than detecting high power jamming attacks. To our knowledge, the detection of low power jamming attacks with little or no impact on Wi-Fi communication is not addressed in the literature yet, contrary to the detection of jamming with significant impact on Wi-Fi communication. Indeed, in [5], [6] and [7] it is shown that a significant power jamming signal can be detected by analysing the spectral occupation, the received power or error indicators and does not require new approaches.

Detecting a weak jamming signal is part of a global security strategy. This can be done only if we are able to detect a very low power jamming signal that means that it can be detected at a significant distance from the jamming source. The monitoring solution can then protect a larger area and countermeasures can be activated from a network area which is not affected by the jamming signal.

Previous works were performed in an anechoic chamber to analyse the feasibility of detecting jamming attacks by supervised classification approaches. These experiments were carried out without any other interferences in the Wi-Fi frequency band and showed that relatively low jamming signals could be detected by SVM classification [8]. However, the same supervised approach, of our previous works, applied on measurement under realistic conditions, i.e. in a place where the use of the spectrum is shared between multiple applications, was not able to discriminate standard communications from communications in the presence of jamming signals [9]. The inability to correctly detect low jamming signals is due to the fact that:

- Other wireless applications which use frequencies in the Wi-Fi band can also disrupt the Wi-Fi communications.
- The power of the jamming signal can be significantly lower than the one of the ambient electromagnetic activity.
- The other communications in the ISM bands are unpredictable and produce an EM environment that is not compatible with a supervised method.

For all these reasons, the detection method should be able to identify intentional jamming among the signals from these other wireless applications that constitute unintentional perturbations.

B. Contribution

This paper aims to detect a jamming that can be extremely weak in a variable and uncontrolled environment. In order to come up with an effective solution in such circumstances, we first want to identify the different communication profiles. In summary, the contributions of this paper are :

- To deploy a monitoring solution only on data at the physical layer, thus enabling a monitoring architecture that is independent of the monitored communication network and respects privacy.
- To treat a very low power jamming (compared to the ambient electromagnetic activity) that has almost no effect on communication and is invisible by direct observation of the spectrum.
- To characterize the different communication profiles in an uncontrolled open environment and detect the possible presence of low power jamming.
- To detect a jamming attack
- To characterize and detect the low jamming based on the study of the physical layer.

C. Organisation

This paper is organized as follows. Section III describes in detail the realistic test conditions that were adopted, the jamming signal characteristics, the Wi-Fi network and the attack configuration. Section IV compares the scope of application of different classification algorithms and highlights the characteristics of the selected one. Section V describes the classification approach used to discriminate different profiles of communication. Section VI is a deep analysis of the frequency contents in both cases (attack and no attack). The section VII analyses the different clusters issued from the classification in order to select the clusters allowing to develop a strategy detection of jamming signals. Finally, section VIII analyses the characteristics of the spectra grouped in the clusters that are significant in the presence or absence of jamming attacks.

III. EM ATTACK EXPERIMENTATION CONFIGURATION

A. Preliminary description of the measurement test site

The experiments analysed in this article were carried out with a wi-Fi network specifically installed in a room of the Gustave Eiffel University. No specific precautions were taken to avoid ambient ISM emissions intended for the activities of the University's staff. Indeed, this building is equipped with various systems using the ISM frequency band (door remote control system, occupancy sensor, Wi-Fi networks...). We only identified in advance the channels the most used by this internal Wi-Fi network to select an unused channel for our test network. We chose the channel located at 2.422 GHz because it was far away enough from the channels used by the university's network and was therefore not likely to disturb them. By conducting our tests in a space that is not protected from ambient emissions, our conditions can vary considerably from one measurement to an other. For example, the activity on the University network can be more or less important, terminals connected to the University Wi-Fi network can be deployed inside the building and be more or less close to the test area. Smart phones can also be activated in a Wi-Fi gateway mode by guests who do not have access to the internal

Wi-Fi network. These Wi-Fi gateways generally scan all the Wi-Fi bands and can use channels that occur to be the same as our test channel. Finally, other devices can also use the Wi-Fi frequency band with a different communication protocol. In these not protected variable conditions, we have observed that the Wi-Fi communications of our test networks are more sensitive to jamming signals than in a protected anechoic environment. The presence of other applications in the Wi-Fi band implies that extremely low jamming power signals can be sufficient to interrupt the Wi-Fi communication. Other ambient communications are observed to act as unintentional interferences and have a superimposed impact on the jamming signal, resulting in a communication failure.

Consequently, the objective is to distinguish the presence of a low power jamming signal that has nearly no effect on the communication, unless another ISM application weakens the Wi-Fi communication.

B. Jamming signals

The attack by jamming signals consists in intentionally emitting a signal which covers the frequency bands employed by a communication system in order to disturb the reception of a communication device. Generally, the power levels of jamming signals are similar to communication signal power levels. The jamming signals can degrade the performance of the communication networks without damaging the communication devices. Different types of jamming signals can be used [10]. The vast majority of commercial jammers uses a cyclic frequency-sweeping interference signal, which sweeps a frequency band $[f_1, f_2]$ in a time duration T. It can be expressed as:

$$s(t) = A\cos\left(2\pi\left(\frac{f_2 - f_1}{2T}t + f_1\right)t\right), \quad 0 < t < T, \quad (1)$$

where A is the interference signal amplitude. Here, the Wi-Fi jamming signal that we consider sweeps the $[2.4\text{ GHz}, 2.5\text{ GHz}]$ frequency band in $T = 10\ \mu$s

The jamming signal waveform defined by (1) is generated with an AWG connected to a variable attenuation control unit in order to reduce the power of the jamming signal and to emulate a jamming source far away from the test site.

According to the wireless communication protocol, the power of the jamming signal required to interrupt the communication and to provoke a deny of service on the application, can vary. As a consequence, depending on the wireless application we want to protect, we must be able to detect more or less powerful interference signals. Previous studies analysing the impact of jamming signals on the Wi-Fi communication have shown that a jamming signal with a power 30 dB lower than the power of the considered Wi-Fi signal can be sufficient to interrupt the communication [10].

C. Device setting

For the experiments, a specific Wi-Fi network was set-up in a room of the university Gustave Eiffel by installing a server, an access point and a client computer. The client computer is equipped with the Iperf network testing tool. Iperf allows creating TCP and UDP data streams and measuring the network throughput. The Wi-Fi channel employed is centered on the 2.422 GHz frequency. The jamming signal is emitted with a small omni-directional antenna connected to the arbitrary waveform generator and the attenuation control unit. The variable attenuation control unit allows adjusting the jamming signal power. We measured the bit rate thanks to the Iperf software, and we increased progressively the power of the jamming signal until we observed a very small impact on the bit rate.

To measure the electromagnetic activity, we placed a monitoring antenna nearby the client. The monitoring antenna is a small omni-directional antenna and is connected to a real time spectrum analyzer (see Fig 1).

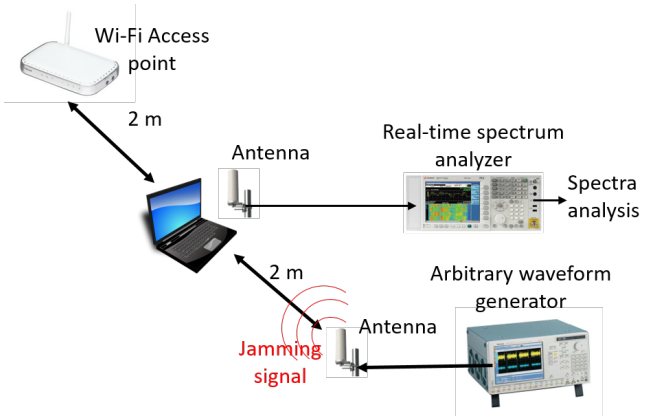

Fig. 1: Experimentation with a 802.11n communication in the presence of jamming attack

A 40 MHz frequency band, centred on 2.422 GHz, is monitored by the spectrum analyzer. Each collected spectrum contains 1601 frequencies measured with a 100 kHz resolution bandwidth and a 38.2 μs sweep time. Each spectrum is obtained in applying the "MaxHold" function of the spectrum analyzer over ten successive scans of the 40 MHz frequency band. That means that for each frequency, the maximal measured power behind the ten previous scans is recorded.

Figures 2 and 3 present ten spectra obtained without jamming signals and in the presence of jamming signals.

These figures show that the jamming signal has such a low power and is nearly invisible in the spectrum pattern. It is impossible to recognize the presence of the jamming signal by visual comparison.

Experiments were performed over two test days and alternating measurements with jamming attacks and measurements without jamming. We collected 10998 spectra without jamming signals and 29996 spectra in the presence of jamming signals.

IV. CLASSIFICATION ALGORITHMS SPECIFICITIES

The purpose of this paper is to characterize communications subject to a low intensity interference as well as to detect them. To do this, from the acquired data, we use data mining and classification techniques. As a first step, it is important to identify different possible approaches to perform this task.

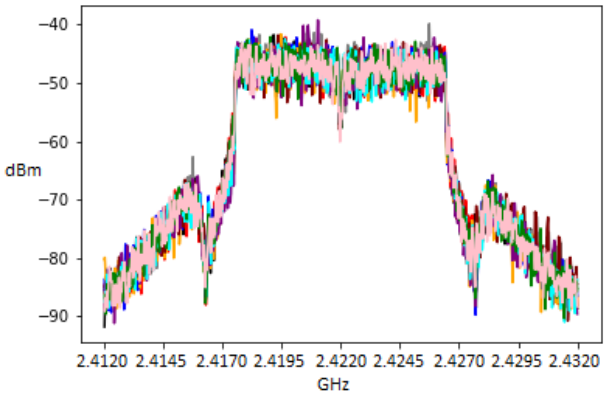

Fig. 2: Ten spectra obtained with Wi-fi signal only.

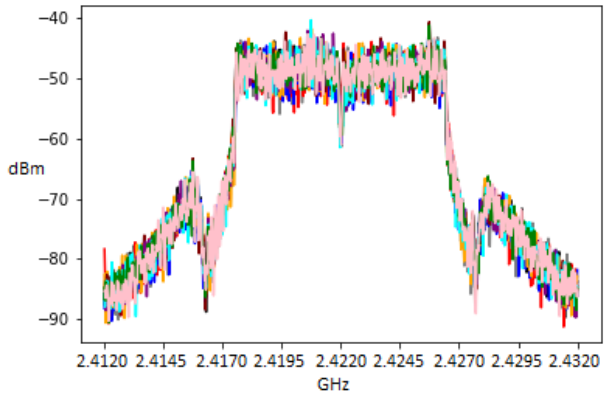

Fig. 3: Ten spectra obtained with Wi-Fi and low power jamming signals.

The compared algorithms are SVM [11], Neural Network [12], Random Forest [13], Decision tree [14], Mixture Model Based Clustering [15], K-means [16] and AHC [17]. To compare these algorithms we are interested in their fields of application. We thus seek to know if the algorithm is supervised, automatic, adaptable and interpretable, as well as its speed and precision. This information is resumed in Table I. In this paper the objectives are at two levels. The first level is to set up a model to characterize different communication profiles. To this end, the classification model must be interpretable, that is to say, it must be possible to obtain an interpretation of the physical characteristics of each profile obtained. The second level is detection. From the profiles obtained, we want to be able to identify which profiles are related to low intensity interference situations. Knowing that spectra by interference are not linearly separable. The use of only two classes does not provide sufficient finesse in the detection of the low-intensity jamming signal. Therefore, we do not know a priori the number of classes of our classification. In order to respect these constraints, we will use, in the following, a AHC combined with a distribution test to discriminate different communication profiles.

V. Agglomerative Hierarchical Classification

A. principle

AHC [17] is an automatic clustering method used in data analysis. Its purpose is to distribute a set Ω of n individuals in a certain number of clusters. The method assumes that there is a measure of dissimilarity between individuals allowing to measure the difference between two entities. The greater this value is, the more the two entities are different. The AHC is sometimes called ascending because it starts from a situation where all the individuals are alone in a cluster, then are gathered in increasingly large ones. Initially, each individual forms a cluster, i.e. n clusters. The algorithm reduces this number to $n_b < n$ by aggregating iteratively (at each step, two clusters are merged).

B. Aggregating rules

At each step of the algorithm, it is necessary to update the distance table. After each grouping of two individuals, two clusters or an individual to a cluster, the distances between this new object and the others are calculated. Different approaches are possible at this level, giving rise to different AHC implementations.The problem is to define $d(A, B)$, distance between two elements of a partition of Ω.The strategies below accommodate a simple index that defines the dissimilarity between individuals.

- $d(A, B) = \min_{\forall i \in A, j \in B}(d_{ij})$ (single linkage)
- $d(A, B) = \max_{\forall i \in A, j \in B}(d_{ij})$ (complete linkage)
- $d(A, B) = \frac{1}{Card(A).Card(B)} \sum_{\forall i \in A, j \in B}(d_{ij})$ (group average linkage)

We can also consider that the data is in the form of an $n \times p$ matrix of quantitative variables associated with a Euclidean metric in $\mathbb{R}^p$ or directly in the form of a matrix of Euclidean distances $(n \times n)$ of 2 by 2 individuals. In this case, it is easy to calculate the center of the classes and to consider the following distances between two groups.

- $d(A, B) = d(c_A, c_B)$ (centroid)
- $d(A, B) = \frac{w_A . w_B}{w_A + w_B} d(c_A, c_B)$ (Ward)

It is also possible to use the similarity such as the correlation for example.

C. Results interpretation

The two closest clusters are merged, in other words, those with the minimum dissimilarity. This dissimilarity value is called the aggregation index. Using this index, it is easy to construct a tree that represents the order and the height of each aggregation. As the closest individuals are gathered first, the first iteration has a low aggregation index or height (see Fig. 4), but it grows from iteration to iteration. When the classes have several individuals, there are multiple criteria which make it possible to calculate dissimilarity. Once these steps are performed, we have to select the desired number of clusters.

	supervised	Automatic	adaptability	interpretable	prediction speed	accuracy	number of cluster
SVM	×				fast	high	fixed a priori
Neural Network	×				fast	high	fixed a priori
Random Forest	×				moderate	high	fixed a priori
Decision tree	×	×			fast	low	fixed a priori
Mixture model based clustering		×	×	×	fast	not concerned	fixed a priori
K-means		×	×	×	fast	not concerned	fixed a priori
AHC		×	×	×	fast	not concerned	fixed a posteriori

TABLE I: Classifcation algorithm comparisons

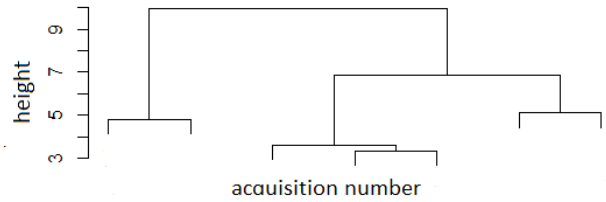

Fig. 4: Dendrogram

D. Number of cluster selection

In order to choose the number of clusters, we can calculate the inter-class distance decrease. The presence of a significant break in this decrease helps in the choice of the number of classes. In our case, we labelize at each step the cluster with the label which has the higher proportion. We estimate the proportion of each label in the studied sample. This proportion is given by

$$P_i = \frac{\text{Card}(\Omega_i)}{\text{Card}(\Omega)} \tag{2}$$

where Card is the cardinality function, Ω is the space of possible cases and Ω_i is the space of favorable cases for the condition i. Once each cluster is labelized, we calculate the classification error given by

$$\epsilon = \sum_{c=1}^{m} \frac{\text{Card}(\Omega_{Fc})}{\text{Card}(\Omega_c)} \tag{3}$$

where Ω_{Fc} is the space of errors in the cluster c and Ω_c is the space of candidates in the cluster c. The presence of a significant break in the decrease in the error determines the number of classes.

E. Cluster effect

Once the number of clusters is determined, we have to determine if the clusters have an effect on the distribution of each label. To determine if the proportion is significantly different from the original partition, we use a statistical test that permits to compare the distributions. To distinguish a difference in proportions between two populations, we check whether this difference follows a normal law of zero mean (therefore centered), this is hypothesis H_0 of the test. If we reduce this difference by dividing it by its standard deviation, we get a random variable which follows a normal law not only centered but reduced.

$$t = \frac{p_1 - p_2}{\sqrt{\frac{p_1(1-p_1)}{n_1}\frac{p_2(1-p_2)}{n_2}}} \tag{4}$$

where p_1 and n_1 are respectively the proportion and the number of cases in the first configuration (here in the cluster) and p_2 and n_2 are respectively the proportion and the number of cases in the second configuration (here a configuration without classification). So we compare the t-value of the reduced centered normal distribution (i.e. 1.96 if we use the classic bilateral confidence interval of 95 %) with this statistic.

VI. Analysis

A. Principal Component Analysis

A way to check if the different classes (with or without jamming) can be separated is to compute a PCA on all data [24]. These principal components correspond to the axes obtained from the eigenvectors constructed from the spectra. Projecting the spectra on the first components associated to the eigenvector possessing the higher eigenvalues, we check if the different configurations can be discriminated by classification. In the PCA representation, each point corresponds to one spectrum. In [8], the experiments were performed in a anechoic chamber (without any other emissions than the Wi-Fi communication and the jamming signal), the PCA and the representation in the two first components showed the separation of the situations with and without jamming. In this present article, we also calculate the PCA over the spectra obtained in a realistic environment with and without jamming signals.

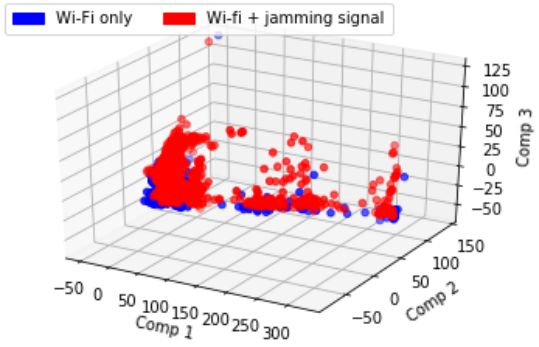

Fig. 5: Representation of the measured spectra on the three eigenvectors / components (comp) associated to the highest eigenvalues

In Fig. 5, we represent the projection of these spectra in the three first components (comp 1, comp 2, comp 3) associated to the eigenvector possessing the higher eigenvalues. We notice

that the Wi-Fi communication alone and the communication plus a low power jamming signal are not perfectly discriminated by their position in the space representation. However, there were times when communication suffered significant drops in flow or even brief interruptions. Nevertheless, these effects were probably the result of other ISM communications or of the superimposition of jamming signals plus another ISM communication. Looking at the distribution of the points, we observe that both situations, with and without jamming, are equally scattered in the space of representation. That shows that certain other ambient ISM emissions can be assimilated to intentional low power jamming in terms of impact. Indeed, by the supervised method, the acquisitions have to be labeled as " with jamming" or "without jamming" but it is not sufficiently precise to distinguish the variety of the realistic conditions due to the presence of other ISM ambient emissions. Due to these, the models constructed in [8] cannot be applied to estimate the state of the communication. Furthermore, Figure 5 shows the difficulties to discriminate a standard communication with the one under a jamming signal. To improve the separation between these classes, we should take into account other components beyond the first two and adopt a nonlinear separation. In order to improve the separation approach, it is important to identify the importance of each frequency on the discrimination between a standard communication and a communication under a jamming attack.

B. Frequency band variance analysis

To analyse the importance of the frequencies, we study the linear relationship between the frequencies of a spectrum. From the spectra obtained, we aim to find frequencies that can distinguish classes corresponding to known attacks. The variance decomposition makes it possible to study the analysis of the variance of Y using the equality of the conditional means of this numerical variable in the sub-populations induced by X. In this problem, X is called the explanatory variable, or the explanatory factor, and Y the explained variable. In the variance decomposition formula,

$$Var_{Tot} = Var_{between} + Var_{within}$$

the variance within class, mean of the variances (conditional), quantifies the share of the intrinsic variability of Y, and the variance between classes, variance of the means (conditional), measures the heterogeneity of the sub-populations.

The spectrum acquisitions are performed over a 40 MHz frequency band. Based on the variance study (6), we highlight the frequencies that have the higher capacity to discriminate the communication. This analysis shows us that the frequencies that give the best values to separate a jammed communication from a standard communication in a linear way, are the frequencies located between $[2.4135,2.41245]$, $[2.4160,2.4165]$ and $[2.4300,4.4320]$ GHz. These frequencies are the ones that give the highest ratio between the variability "between the classes" and the variability "within the classes". We notice that the frequency bands providing the best discrimination capability are not in the 20 MHz communication channel. It shows the importance of monitoring a frequency band wider than the frequency band used by the Wi-Fi communication channel.

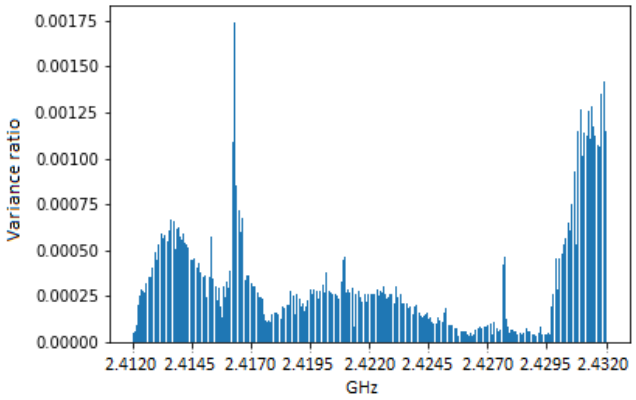

Fig. 6: Variance ratio for each frequencies.

VII. Classification results

A. AHC

For the classification of the spectra, we use an automatic classification algorithm that allows the interpretation of the results. To analyse the Wi-Fi communications, we generate, using AHC algorithm, different clusters of homogeneous communication. The AHC is performed using the Ward's criterion. To select the number of clusters, we use the classification error induced by associating to a cluster the label of the most representative case. Here, the case is the presence or the absence of a jamming signal in the communication (see Fig 7). Once the number of 8 clusters has been exceeded, the classification error does not change significantly by increasing the number of clusters. For this reason, we analyse the spectra of these 8 clusters.

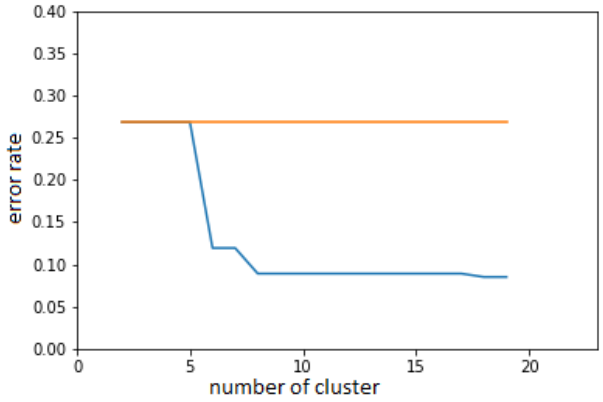

Fig. 7: Evolution of the classification errors according to the number of cluster.

B. Proportion analysis

Once the 8 clusters have been defined, we analyse the distribution of Wi-Fi communication with or without jamming

signals in each cluster in order to study the relevance of these clusters to develop a jamming attack detection strategy. To determine if each cluster has an impact in the characterization of the communication, we need to check if the proportion of communications with or without jamming signals corresponds to the one obtained when no classification is performed. The table VII-B contains the number of spectra of each cluster as well as the proportion of Wi-Fi communication only and Wi-Fi in presence of jamming signals in the cluster. To determine if the proportion is significantly different from the original partition, we use a statistical test that permits to compare the distributions. Here p_1 corresponds to the proportion of communication without jamming and p_2 corresponds to the communication under a law jamming signal.

cluster	Wi-Fi only	Wi-Fi + jamming
1	27 / 23%	91 / 77%
2	0 / 0%	122 / 100%
3	50 / 27%	125 / 73%
4	123 / 25%	366 / 75%
5	1019 / 31%	2259 / 69%
6	8304 / 90%	962 / 10%
7	65 / 2%	3983 / 98%
8	1410 / 6%	22088 / 94%
Sum	10998 / 27%	29996 / 73%

TABLE II: Cluster distribution

The clusters highlighted in green in table VII-B represent the clusters with a significant difference of proportion in relation to the global distribution of communications with or without jamming. In consequence, these results reveal that the clusters 3 and 4 have no effect on the distribution of the spectra. This means that whether or not there is a jamming signal, the distribution within these clusters is the same as the proportion within the data set. In these cases, the resulting distribution can not allow us to detect the jamming signal. Regarding the clusters 1 and 5, the distributions are slightly different from the original distribution. But the difference is not obvious enough to affirm that this cluster characterizes a communication under intentional jamming signals. The clusters that have a significant difference in the distribution, in relation to the original partition, are the clusters 2, 6, 7 and 8. The clusters 2, 7 and 8 contain a significant proportion of spectra with jamming while cluster 6 is mainly composed of spectra without jamming. In the next section, we therefore precisely analyze these 4 clusters that can be used to design a low-power jamming signal detection method.

VIII. Cluster profiling

The Figure 8 represents the spectra position of the 8 clusters in the space corresponding to the three eigenvectors associated to the three strongest eigenvalues. This representation permits to highlight the difference between the different clusters in a transformed space which represents the different frequencies of the spectra. We notice that the clusters 1 and 3 are well separated in the space from the other clusters. Nevertheless, the distributions with or without jamming attacks in these two clusters are not different from the distribution in the acquired data. Thus, although they are easily separable from other clusters, they cannot be used for jamming attack detection. Looking at the clusters 2, 6, 7 and 8, which are interesting for detection, we can see that they are all clustered in the same part of the space and they are difficult to separate.

In the following, we analyse in detail the spectra that compose different clusters to better understand their differences. Firstly, we analyse the cluster 6 which is characteristic of the absence of a jamming attack. Then, we analyse clusters 1 and 5 which illustrate useless clusters. Finally, we analyse clusters 2, 7 and 8 which are significant to detect the presence of a jamming attack. This analysis contributes to optimize the acquisition mode in terms of sweep time, frequency resolution, Maxhold or real time in order to accentuate the capability of differentiating them.

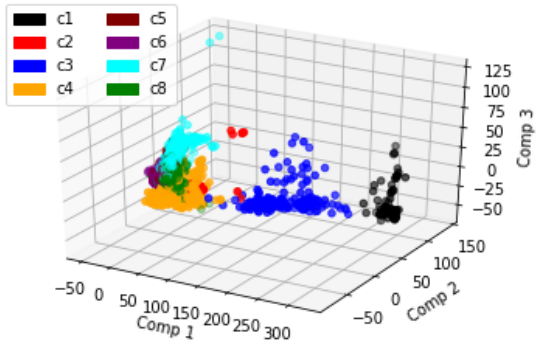

Fig. 8: Class distribution on the 3 dimensions corresponding to the eigenvectors / components (comp) associated to the highest eigenvalues.

The spectra represented in figure 9 correspond to cluster 6 and characterize a Wi-Fi communication without attack. The spectra represented on figures 10 and 11 correspond to spectra contained in clusters 1 and 5 that can not be used to distinguish the presence or the absence of jamming signals. Finally, figures 13, 14 and 15 characterize spectra of Wi-Fi communication with jamming signals. In these figures, the blue lines represent the minimum, mean and maximum values for each frequency. The black lines represent the spectra of the Wi-Fi communications in the presence of intentional jamming signals and the grey lines represent the spectra of the Wi-Fi communications without intentional jamming signals.

For cluster 6 (see Fig. 9), the spectra are typical representations of Wi-Fi communications correctly transmitted without any alteration on the 20 MHz Wi-Fi channel, located between 2.417 and 2.427 GHz. In this cluster, 90% of the spectra are obtained without jamming signals. On the 20 MHz channel, the power level is stable for each spectrum with a level between -40dBm and -55dBm, giving a variability of about 15 dB. On the bands located in the interval of frequencies [2.412, 2.416] GHz and [2.428, 2.432] GHz, we notice the same variability of about 15 dB between the maximal and

minimum values.

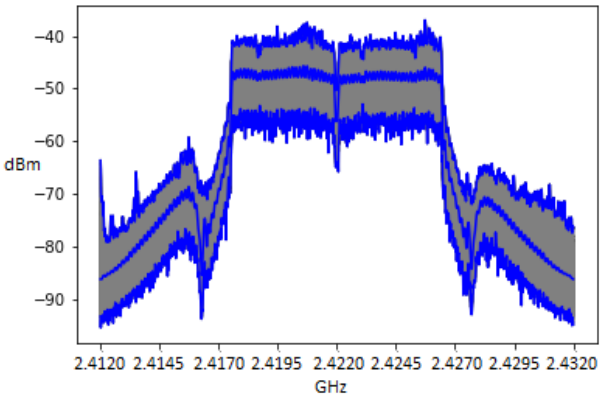

Fig. 9: Spectra in cluster 6.

Looking at the cluster 1 spectra, we observe that it corresponds to the absence of Wi-Fi communication, in the presence of jamming or not. Here what dominates is not the presence of jamming, but the fact that there is no Wi-Fi communication. Thus, this cluster does not bring information on the presence or absence of jamming, as is the case of cluster 5. Cluster 5 corresponds to Wi-Fi preamble spectra.

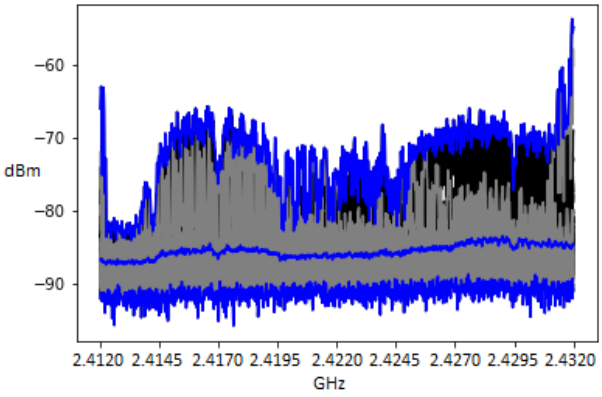

Fig. 10: Spectra in cluster 1.

The Wi-Fi preamble is composed of two fields [26]: a short training field, consisting of 10 repetitions of a periodic short training signal, and a long training field, which includes two repetitions of a given periodic training signal. The signal for the short training field is modulated by transmitting on only one subcarrier out of four, yielding 12 modulated subcarriers. Let us recall that when transmitting data, Wi-Fi modulates 48 subcarriers out of 64, the rest being used as guard subcarriers. This can be easily observed on Fig. 11 where the peaks correspond to the 12 subcarriers used by the preamble. For further illustration, a time-frequency representation of a Wi-Fi transmission recorded during the measurements is also shown in Fig. 12. The Wi-Fi frame starts with the preamble, identified in the frequency domain by its sparse subcarriers. Similarly to cluster 1, cluster 5 is not dominated by the presence or

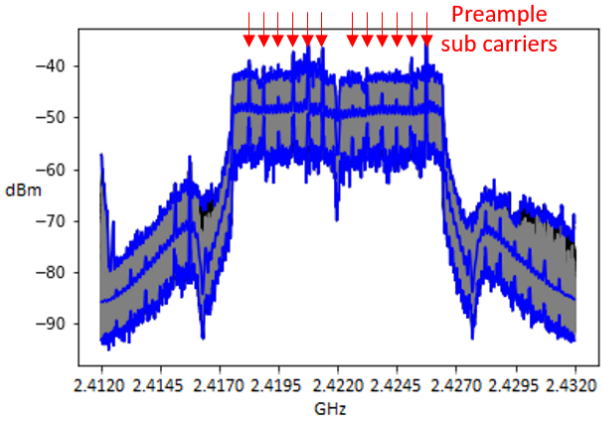

Fig. 11: Spectra in cluster 5.

absence of jamming signals but by a specific pattern which is the preamble, contrary to clusters 2, 7 and 8 which are presented hereafter.

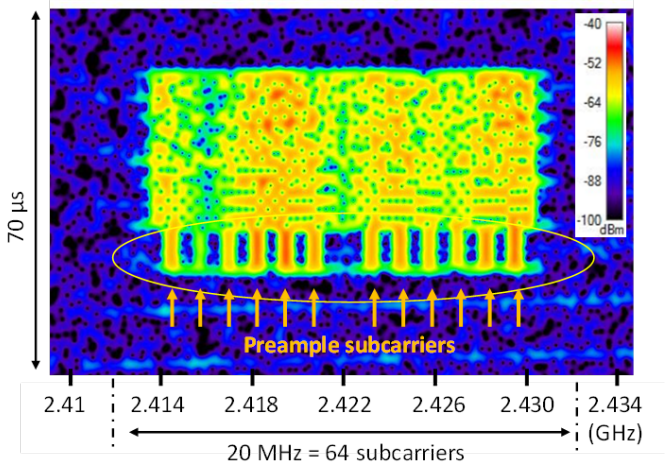

Fig. 12: Time-frequency representation of a Wi-Fi communication

Clusters 2, 7 and 8 contain a significant majority of acquisitions in the presence of a jamming signal. By analysing the spectra composing these three clusters, we can then identify the characteristics which allow to build an attack detection strategy.

All the spectra included in cluster 2 are obtained during experiments in the presence of intentional jamming signals.

The cluster 2 spectra, presented in fig. 13, has a very specific shape. This shape is characteristic of the probe signals sent by the client computer. Indeed, when a client computer is not able to listen any beacon signal generated by the access point, the computer sends probe signals (IEEE Wi-Fi signalling frames [27]) containing the name of the BSSID (Basic Service Set IDentifier) which is the name of the wireless network [27]) already known (from previous connections). These probes permit to the computer to start the authentication and association process to the access point. Knowing that all the cluster 2 spectra belong to tests performed in the presence

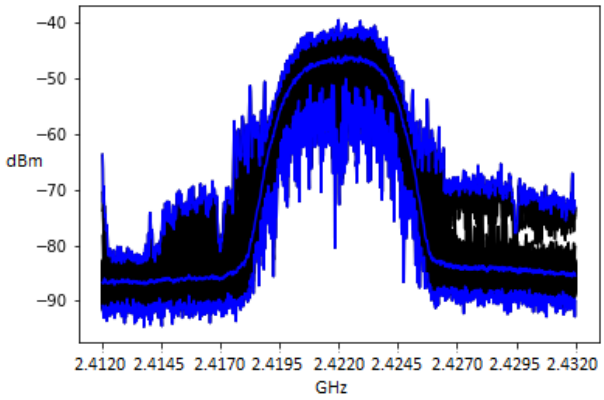

Fig. 13: Spectra in cluster 2.

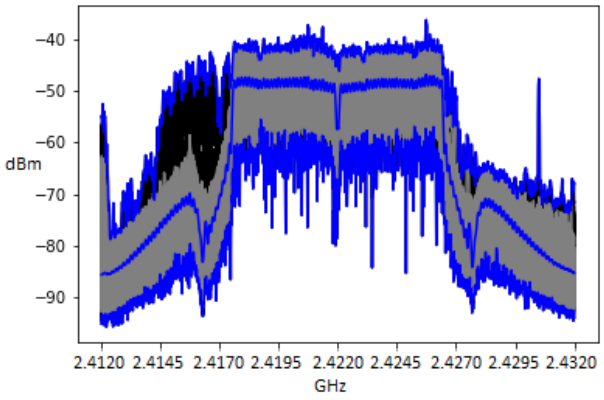

Fig. 15: Spectra in cluster 8.

of jamming signals, it seems that this probe sending process is mainly activated when a jamming signal is acting.

Clusters 7 and 8 are respectively composed by 94% and 98% of spectra obtained in the presence of intentional jamming signals. Both clusters are then characteristics of the presence of attacks by jamming. Presented in Fig. 14 and 15, we observe that the spectra composing these clusters totally occupy the 20 MHz of the central part. That means that Wi-Fi communications are in operation during the acquisitions. Then, unlike the cluster 2, these clusters 7 and 8 can allow to detect the presence of jamming attacks even if the Wi-Fi communications are operating without any alterations.

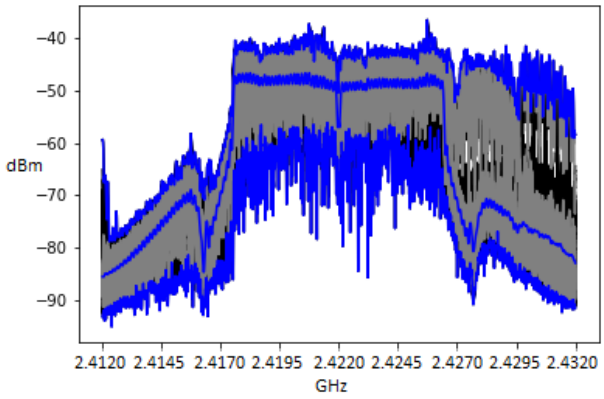

Fig. 14: Spectra in cluster 7.

The comparison of the clusters 7 and 8 spectra with the cluster 6 spectra can allow to identify the characteristics used to detect the presence of low power jamming signals. Firstly, we notice differences in the 20 MHz central frequency band. Indeed, clusters 7 and 8 have a greater variability in the 20 MHz central part because the minimum power values are much lower than those of cluster 6. We also notice that the cluster 7 has a higher variability in the right part of the spectra, for frequencies above 2.427 GHz, while the cluster 8 has a higher variability in the left part, for frequencies below 2.418 GHz. Moreover, fig. 6 highlights the importance of frequencies on either side of the channel for discrimination of the communication. In consequence, it appears that the spectra of clusters 7 and 8 are grouped together due to the variability between the successive data forming the spectra. This can be explained by the fact that the presence of the jamming signal induces a higher instability of the Wi-Fi communications, then contributing to more frequent variations of the spectral occupation.

IX. Conclusion

This study aims to detect very weak jamming signals, perfectly indistinguishable by a visual analysis of the frequency spectrum, and performed in a shared environment in terms of wireless communications.

The first part of the study analyses the frequencies which are the most affected by a weak intentional jamming signal. It shows the importance of the neighbour frequencies of the 20 MHz Wi-Fi channel to discriminate the presence of a jamming signal and the importance to monitor a wider frequency band than the 20 MHz frequency band occupied by Wi-Fi communications.

Then, a deeper analysis using a clustering approach permits us to characterise the different spectral occupation situations observed in an open environment in which we have no control on the wireless communication activity. This analysis identifies the discriminant clusters with a proportion of spectra, with or without jamming signals, significantly different from the whole data set distribution. It allows us to conclude that the profiles making it possible to identify the presence of a jamming signal with the highest efficiency are spectra that correspond to a probe signal and spectra with a high variability in the frequency bands corresponding to the most discriminant frequencies. We can then optimize the parameters of the acquisition process in order to increase the visibility of this variability.

In future works, new acquisition campaigns will be conducted in different areas in order to verify if the conclusions concerning the discriminant clusters can be generalized. Moreover, a next analysis will focus on the chronology of these profiles to assess the laps of time required for a more robust attack detection.

ACKNOWLEDGMENT

This work was performed in the framework of the EL-SAT2020 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] Z. Lu, W. Wang and C. Wang, *Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications*, in IEEE Transactions on Mobile Computing, vol. 13, no. 8, pp. 1746-1759, Aug. 2014.

[2] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, G. Nauryzbayev, X. Li and R. Kharel, *Towards Physical Layer Security for Internet of Vehicles: Interference Aware Modelling*, IEEE Internet of Things Journal, 2020.

[3] J. Wang, C. Jiang, H. Zhang, Y. Ren, K. C. Chen and L. Hanzo, *Thirty years of machine learning: The road to Pareto-optimal wireless networks*, IEEE Communications Surveys & Tutorials, 2020.

[4] S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao, Y., H. Zhou, *Delimitated anti jammer scheme for Internet of vehicle: Machine learning based security approach*, IEEE Access, 7, 113311-113323, 2019.

[5] G. Liu, J. Liu, Y. Li, L. Xiao and Y. Tang, *Jamming Detection of Smartphones for WiFi Signals*, 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, pp. 1-3, 2015.

[6] W. Xu, W. Trappe, Y. Zhang, and T. Wood, *The feasibility of launching and detecting jamming attacks in wireless networks*, in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, ACM, pp. 46–57, 2005.

[7] R. Bhojani and R. Joshi, *An integrated approach for jammer detection using software defined radio*, Procedia Computer Science, vol. 79, pp. 809–816, 2016.

[8] J. Villain, V. Deniau, A. Fleury, E. P. Simon, C. Gransart, R. Kousri, *EM Monitoring and classification of IEMI and protocol-based attacks on IEEE 802.11 n communication networks*, IEEE Transactions on Electromagnetic Compatibility, 2019.

[9] J. Villain, A. Fleury, V. Deniau, C. Gransart, E. Simon, *Online EM Monitoring of 802.11 n Networks using Self Adaptive Kernel Machine*, 18th IEEE International Conference On Machine Learning And Applications (ICMLA), pp. 1136-1142, IEEE, 2019.

[10] V. Deniau, C. Gransart, G. L. Romero, E. P. Simon, and J. Farah, *IEEE 802.11n Communications in the Presence of Frequency-Sweeping Interference Signals*, IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 5, pp. 1625–1633, 2017.

[11] V. Vapnik, *The nature of statistical learning theory*, Red Bank: Springer, vol. 2, 2000.

[12] C. M. Bishop, *Neural Networks for Pattern Recognition*, Oxford University Press, 1995.

[13] L. Breiman, *Random forests*, Machine learning, 45(1), pp. 5-32, 2001.

[14] K. Karimi, H.J. Hamilton, *Generation and Interpretation of Temporal Decision Rules*, International Journal of Computer Information Systems and Industrial Management Applications, Volume 3, 2011.

[15] K. Ozonat, R. M. Gray, *Gauss mixture model-based classification for sensor networks*, In Data Compression Conference, pp. 322-331, IEEE, March 2006.

[16] J. B. MacQueen, *Some Methods for classification and Analysis of Multivariate Observations*, Proceedings of 5th Berkeley Symposium on Mathematical Statistics and Probability, 1, University of California Press, pp. 281–297, 1967.

[17] T. Hastie, R. Tibshirani, J. Friedman, *Hierarchical clustering*, The Elements of Statistical Learning (2nd ed.), New York: Springer. pp. 520–528, 2009.

[18] D. Güsmüsbas, T. Yildirim, A. Genovese, F. Scotti, *A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems*, IEEE systems journal, 2020.

[19] *Electromagnetic compatibility (EMC) - part 2-13: Environment - high-power electromagnetic (HPEM) environments - radiated and conducted*, IEC Standard, Tech. Rep. 61000-2-13 Ed. 1, 2005.

[20] L. Breiman, *Random forests*, Machine Learning, 45, 5–32, 2001.

[21] L. Breiman, *Bagging predictors*, MachineLearning, 26, 2, 123– 140, 1996.

[22] Y. Freund, R.E. Schapire, *Experiments with a new boosting algorithm*, Machine Learning : proceedings of the Thirteenth International Conference, Morgan Kaufman, San Francisco, p. 148–156, 1996.

[23] L. Breiman, *Arcing classifiers*, Annals of Statistics, 26, 801–849, 1998.

[24] S. Wold, K. Esbensen, and P. Geladi, *Principal component analysis*, Chemometrics and intelligent laboratory systems, vol. 2, no. 1-3, pp. 37–52, 1987.

[25] P. Cortez and M. J. Embrechts, *Using sensitivity analysis and visualization techniques to open black box data mining models*, Information Sciences, vol. 225, pp. 1–17, 2013.

[26] document IEEE Std 802.11n-2009, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amen 5: Enhancements for Higher Throughput*, 2009.

[27] IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), *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*, 2007.

Jonathan Villain received the Ph.D. degree in applied Mathematics from the University of Bretagne-Sud, Vannes, France, in 2016 in a French Laboratory of mathematic (LMBA, Vannes) and a Pharmaceutical Laboratory (CERMN, Caen). During 2015 and 2017, he was a Teaching Assistant at the IUT of Vannes. His research field include machine learning and pattern recognition modeling in pharmaceuticals toxicity and cyber-security. As a Postdoctoral fellow at Railenium test and research center and at IMT Lille Douai he participates to WP8 Shift2Rail programs and ELSAT2020 project2020 by studying classification models of electromagnetic disturbances in the transport. He is actually attach to University Gustave Eiffel to continue is study on the ELSAT2020 project.

Virginie Deniau received the M.S. and Ph.D. degrees in electronics from the University of Lille in 2000 and 2003, respectively. Since 2003, she is Researcher in electromagnetic compatibility (EMC) for the University Gustave Eiffel. She conducts works on electromagnetic compatibility (EMC) for land transport. Her research interests include EMC test facilities and methodologies, characterization and modeling of electromagnetic transport environments and the immunity test methodologies for embedded systems. Currently, she works in the hardening of land transport systems regarding cyberattacks, such electromagnetic attacks. She has participated in numerous national and European projects and she was scientific coordinator of the Eu project SECRET for SECurity of Railways against Electromagnetic aTtacks. She is vice-chair of the URSI Committee E (Electromagnetic Interference).

Anthony Fleury (IEEE S'2005, M'2008) is associate professor at IMT Lille Douai. He received an Engineer (Computer Science) and a M.Sc. (Signal Processing) degree in 2005 in Grenoble and a PhD degree in Signal Processing from the University Joseph Fourier of Grenoble in 2008 for his work on Health Smart Homes and activity recognition. He joined then the LMAM team at Swiss Federal Institute of Technology and is now, became, in sept. 2009, Associate Professor at Ecole des Mines de Douai (now IMT Lille Douai). His research interests include modeling human behaviors and activities, machine learning and pattern recognition with applications to biomedical engineering and to security.

Eric P. Simon received the Master's degree in electronics engineering from the Superior School of Electronics (ESCPE), Lyon, France, in 1999, and the Ph.D. degree in signal processing and communications from the National Polytechnic Institute of Grenoble (INPG), France, in 2004. During 2005, he was a Teaching Assistant at the INPG and the following year he joined one of France Telecom R&D Laboratories as a Postdoctoral Fellow. He is currently an Associate Professor at the Institute of Electronics, Microelectronics and Nanotechnology (IEMN), TELICE (Telecommunications, Interference and Electromagnetic Compatibility) Group, University of Lille, France. His main research interests are in mobile communications and carrier and symbol synchronization.

Christophe Gransart received the Ph.D. degree from the University of Lille, Villeneuve-d'Ascq, France, in 1995. He is a Senior Researcher with French Institute of Science and Technology for Transport, Development, and Networks, Villeneuve d'Ascq, with 15 years experience in participating in industrial and academic research projects dealing distributed systems and middleware for transportation systems, V2V and V2I communications, adaptive middleware and cybersecurity. He was involved in various national and European projects. The main competencies are computer science, distributed architecture design, and middleware expertise. He participated to FP6, FP7, H2020, Shift2Rail programs.