SECRET

SECurity of Railways against Electromagnetic aTtacks

Grant Agreement number: 285136
Funding Scheme: Collaborative project
Start date of the contract: 01/08/2012
Project website address: http://www.secret-project.eu

Deliverable D 3.3

"Detection model" for classification and recognition EM attack status

Deliverable on "synthesis model" for experimental simulation of normal and attack conditions: methodology and results
Date: 29/08/2014
Distribution: PU
Manager: IFSTTAR

Document details:

Title	"Detection model" for classification and recognition EM attack status
Workpackage	WP3
Date	28/08/2014
Author(s)	D. Sodoyer, S. Mili, S. Ambellouis, V. Deniau, M. Heddebaut
Responsible Partner	IFSTTAR
Document Code	"Detection model" for classification and recognition
Version	B
Status	Final internal IFSTTAR version (to be externally reviewed)

Dissemination level:

Project co-funded by the European Commission within the Seventh Framework Programme

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission) Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document history:

Revision	Date	Authors	Description
A1	25/07/2014	S. Mili, S. Ambellouis	Chapter 4 Detection of EM attacks by IQ quadratic signals
A2	25/08/2014	D. Sodoyer	First full version
A3	26/08/2014	V. Deniau	Reviewing chapters 2,3 and 4
A4	27/08/2014	M. Heddebaut	Adding some complementary elements
A5	27/08/2014	V. Deniau, D. Sodoyer	Reviewing chapter 5
A6	28/08/2014	M. Heddebaut, V. Deniau	Internal review of the whole document

Table of contents

1. Executive summary 5

2. Introduction 5

2.1. Purpose of the document 5

2.2. Definitions and acronyms 6

3. Ground to train communication based on GSM-R 7

4. Detection of EM attacks based on the IQ quadratic signals 7

4.1. Introduction 7

4.2. Impact of jamming signals on the I/Q constellation 9

4.3. Definition of the descriptors 10

4.3.1. Descriptor 1: radius of the points which composed the I/Q constellation 10

4.3.2. Descriptor 2: Error Vector Magnitude (EVM) 11

4.4. Modelling of the 'normal' operating mode 12

4.5. EM attack detection 14

4.6. Results 15

4.6.1. Description of the measurement configuration 15

4.6.2. Results of the detection with the EVM_{rms} descriptor 16

4.6.3. Results of the detection with the TT(t) descriptor 19

4.7. Conclusion 20

5. Detection of attacks in spectral space 21

5.1. Railway critical environments to be considered 21

5.1.1. Railway line 21

5.1.2. Station 21

5.1.1. Train 21

5.1.2. Results of in situ measurement campaigns 21

5.2. Analysis of the EM environment 22

5.2.1. Introduction and context 22

5.2.2. Analysis and characterization of the EM environment in normal conditions 22

5.2.2.1. Analysis of distributions of p.s.d. according to the measurements sites and the frequency bandwidths 22

5.2.2.2. Analysis of distributions of p.s.d. according to the frequency channels 26

5.3. Definition of the EM statistical Model 32

5.4. Detection procedure of the EM attack 33

5.4.1. Frequency local detection 33

5.4.2. Global detection 34

5.4.3. Integration time detection 34

5.5. Tests and results 35

5.5.1. Methodology 35

5.5.1.1. Learning and test data set 35

5.5.1.2. Perturbation definition 35

5.5.2. Detection results 36

5.5.2.1. Large Band perturbations 37

5.5.2.2. Narrow Band perturbations 37

5.5.2.2.1. LGV line tests 37

5.5.2.2.2. IRIS train tests 38

5.5.2.2.3. Paris Gare de l'Est station 39
5.5.2.2.4. Liège Guillemins station 39
5.5.3. Results conclusion 40

6. Conclusion 41

7. Acknowledgements 41

8. References 41

1. Executive summary

In deliverable D3.3, research activities concerning SECRET tasks 3.3 and 3.4 are described and their results are analyzed. These tasks aim at identifying electromagnetic (EM) attacks to then insure the efficient resilience of the railway system by providing a reconfigurable radio architecture studied in WP4. In a first part, we analyse the In phase and Quadrature phase (I/Q) information accessible in any digital transmission receiver in presence of jamming signal in order to develop an EM attack detection method based on the I/Q information distortions. In a second part, an EM attack detection based on a frequency domain analysis is performed. Each EM attack has a specific representation in the frequency domain, we study how to cluster this frequency domain into several classes related to sub-sets of EM attacks with common properties.

2. Introduction

2.1. Purpose of the document

To detect an anomaly, in our case a jamming condition, aims at finding something that is not consistent with what we expect of the behavior of a system or the behavior of one of its elements. The expected behavior of a system can be defined by its normal state; the occurrence of an anomaly can make the system switch to a degraded state. The detection of an anomaly can be performed using a recognition system.

Therefore, our EM attack detection is built using a recognition system tuned for different types of EM attacks. The detection principle uses supervised pattern recognition techniques. Based on this strategy, different approaches are distinguished and studied in this deliverable.

The first approach consists in performing detection using the train or ground receiving equipment itself. This equipment could be the receiver of a GSM-R transceiver, a TETRA receiving equipment....). To identify the presence of a jammer, we collect the I/Q information directly inside the existing equipment, at different stages along the receiving chain and we develop a specific signal processing to detect EM attacks. We select and study two different descriptors. The first descriptor is represented by the radius of the points which composed the I/Q constellation. The second descriptor exploits the Error Vector Magnitude (EVM) also used to evaluate quality parameters of a radiocommunication. The recognition system is then developed successively using these two descriptors.

The second approach is conducted in parallel with the existing receiving chain. We perform the detection of attacks by an adapted frequency analysis based of the previous knowledge of the normal electromagnetic environments corresponding to the system in use. It uses power spectral densities (p.s.d., expressed in dBm) obtained using a dedicated measuring equipment connected to the same antenna than the corresponding receiver. These p.s.d. are composed of M spectral channels sampled over a bandwidth defined by the frequency selectivity of the antenna, or by the configuration of acquisition system.

2.2. Definitions and acronyms

	Meaning
AWGN	Additive white Gaussian noise
BTS	Base Transceiver Station
p.s.d	Power spectral density
EIRENE	European Integrated Railway Radio Enhanced Network
EM	ElectroMagnetic
ERTMS	European Railways Traffic Management System
ETCS	European Train Control System
EVM	Error Vector Magnitude
FA	False Alarm
GD	Good Detection
GMM	Gaussian mixture model
GSM	Global System for Mobile communications
GSM-R	Global System for Mobile communications - Railways
HSL	High Speed Line
LGV	Ligne à Grande Vitesse (High Speed Line - HSL)
ROC	Receiver Operating Characteristics
SJR	Signal-to-Jamming Ratio
SNR	Signal-to-Noise Ratio
TGV	Train à Grande Vitesse (High Speed Train – HST)

3. Ground to train communication based on GSM-R

GSM-R is a standard communication platform for railway system. It is a strategic communication system focused on interoperability between European railway infrastructures. By the end of 2016, 56 countries in five continents should have operational GSM-R network. Europe is leading GSM-R implementation through mainly 11 countries.

The main objectives of GSM-R are to replace analogical radio communication (RST Radio Sol Train, ground to train radio telecommunications network) and to provide data transmission solution for ERTMS/ETCS (European Rail Traffic Management System / European Train Control System) level 2 and level 3.

GSM-R is an evolution of public GSM standard dedicated to railway application. Therefore GSM-R has similar characteristics than public GSM system.

A common European frequency band is allocated to GSM-R below the frequencies of the public GSM standard. The allocated frequency bands are:

For the uplink (train to Base Transceiver Station):	876 MHz - 880 MHz
For the downlink (Base Transceiver Station to train):	921 MHz - 925 MHz

These two frequency bands will be considered to study the normal electromagnetic (EM) conditions of railway environments. Moreover, to take into account potential extensions of these frequency bands, wider frequency ranges will be considered during the definition of normal electromagnetic environments in chapter 5.

The GSM-R network is designed to provide a minimum level of received power > -95 dBm, this is a mandatory requirement coming from the EIRENE (European Integrated Railway Radio Enhanced Network) specifications [1]. This represents a limited level of power with the potential of being jammed.

4. Detection of EM attacks based on the IQ quadratic signals

4.1. Introduction

In this section, we analyse the In phase and Quadrature phase (I/Q) information accessible in any digital transmission receiver in presence of jamming signal in order to develop an EM attack detection method based on the I/Q information distortions. Then, the detection approach exploits the estimation of I(t) and Q(t) baseband signals obtained after filtering by the chain of demodulation at the level of a GSM/GSM-R receiver.

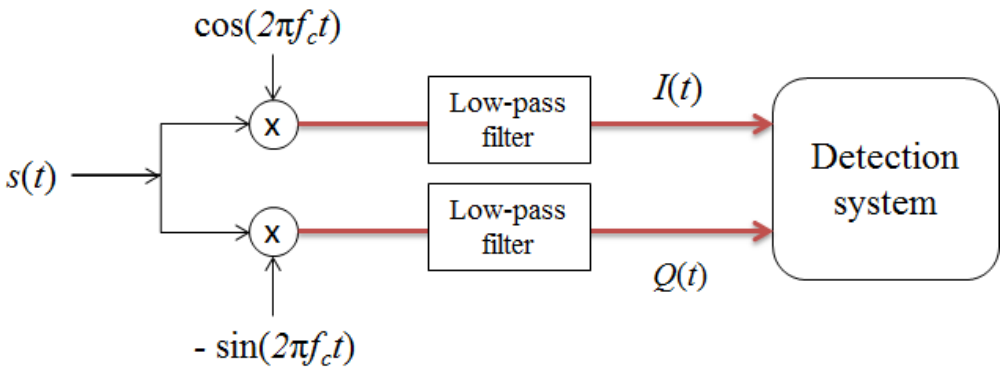


Figure 1 Quadratic detection system

Considering an AWGN transmission channel, I(t) and Q(t) can be expressed by the following equations:

$$I(t) = g(t) * \left(\cos(2\pi f_c t) s(t)\right) \quad (1)$$

$$Q(t) = g(t) * \left(\sin(2\pi f_c t) s(t)\right) \quad (2)$$

I(t) and Q(t) are quadratic estimated signals at reception, while i(t) and q(t) are the quadratic signals at the emission level. For a sampling rate Te of one sample per symbol, the representation of Q(nTe), as a function of I(nTe), is a constellation of the different states of the symbols.

Figure 2 presents such a GMSK constellation for I(nTe) and Q(nTe) signals obtained before and after transmission in a Additive white Gaussian noise (AWGN) channel. The AWGN channel was defined to have a 30 dB Signal-to-Noise Ratio (SNR). By increasing the number of samples, the constellation turns into a circle describing the evolution of quadrature signals. Figure 3 presents I/Q signals with a sampling of 4 samples per symbol.

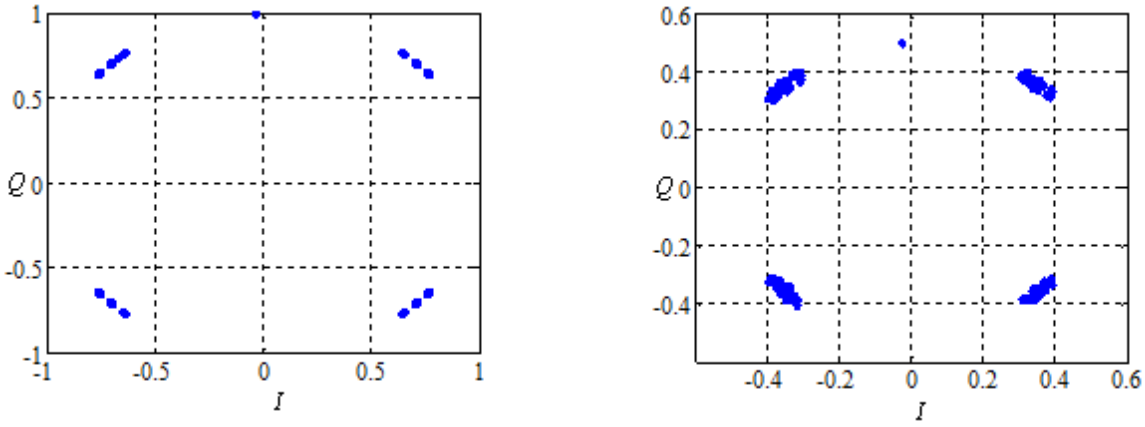


Figure 2. Example of I(nTe) and Q(nTe) signals constellation obtained for a GMSK modulation with a 156 symbols burst before and after AWGN channel with a SNR = 30 dB - 1 sample per symbol.

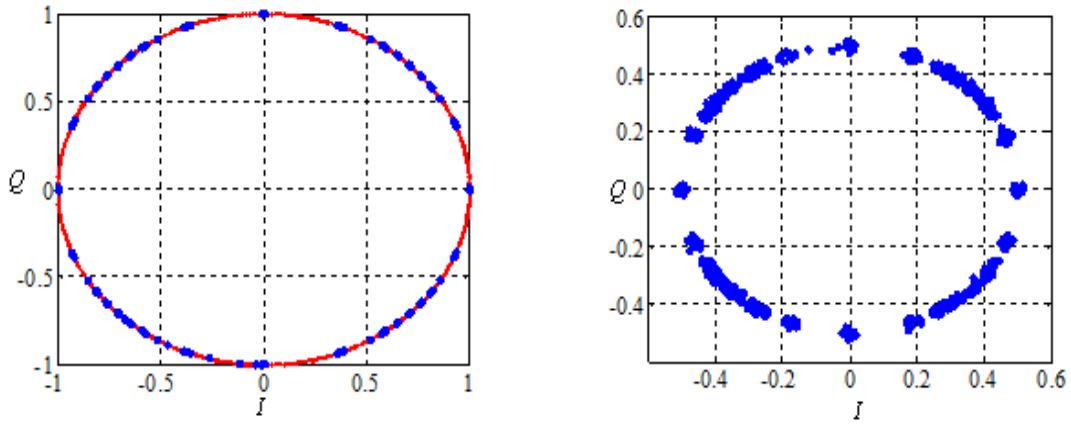


Figure 3. Example of I(nTe) and Q(nTe) signals constellation obtained for a GMSK modulation with a 156 symbols burst before and after AWGN channel with a SNR = 30 dB – 4 samples per symbol

Without AWGN, the constellation forms a perfect circle, centered in 0. AWGN impacts the constellation in dispersing the points on either side of the circle radius. The variance on the point positions is related to the AWGN power.
From this representation, we characterize 'normal' environment of communication in presence of AWGN channel. That means that the distortion induced by the AWGN is considered as a distortion which can be obtained in normal railway operational conditions, without jamming signals.

4.2. Impact of jamming signals on the I/Q constellation

We studied the distortion involved by a jamming signal on the I/Q constellation. Two types of jamming signals were considered:

- $G_1(t)$ a pure sine signal centred in the communication channel and,
- $G_2(t)$ a sine signal with modulation bandwidth of 75 kHz around the carrier frequency.

The impacts of both jamming signals on the constellations are presented Figure 4 and Figure 5.

In these figures, the results are given for two different ratios between the powers of communication and jamming signals (SJR signal-to-jamming ratio).

We notice that the pure sine jamming signal induces a translation of the constellation while a modulated sinusoidal signal increases the scattering of the points on either side of the circle radius.

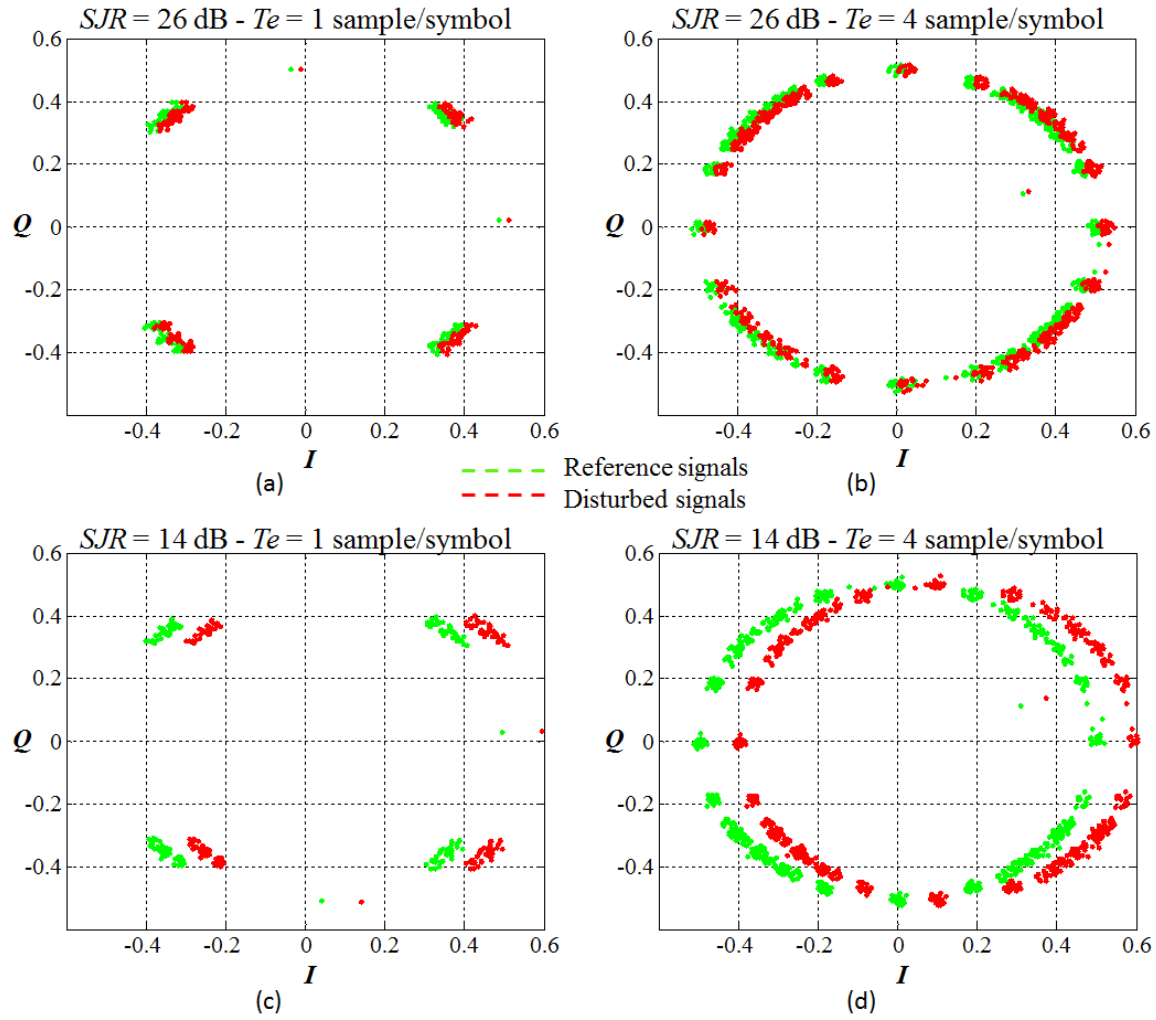


Figure 4: Constellations of signal I(nTe) and Q(enT) estimated at the receiver after transmission in an AWGN channel of SNR = 30 dB and disrupted by a sinusoidal signal of frequency equal to the frequency of the GMSK modulation for SJR = 26 dB (a, b) and SJR = 14 dB (c, d). The constellations are presented for two sampling values: T = 1 sample per symbol (a, c) and T = 4 samples per symbol (b, d). The reference signal is in green and the jammed signal is in red.

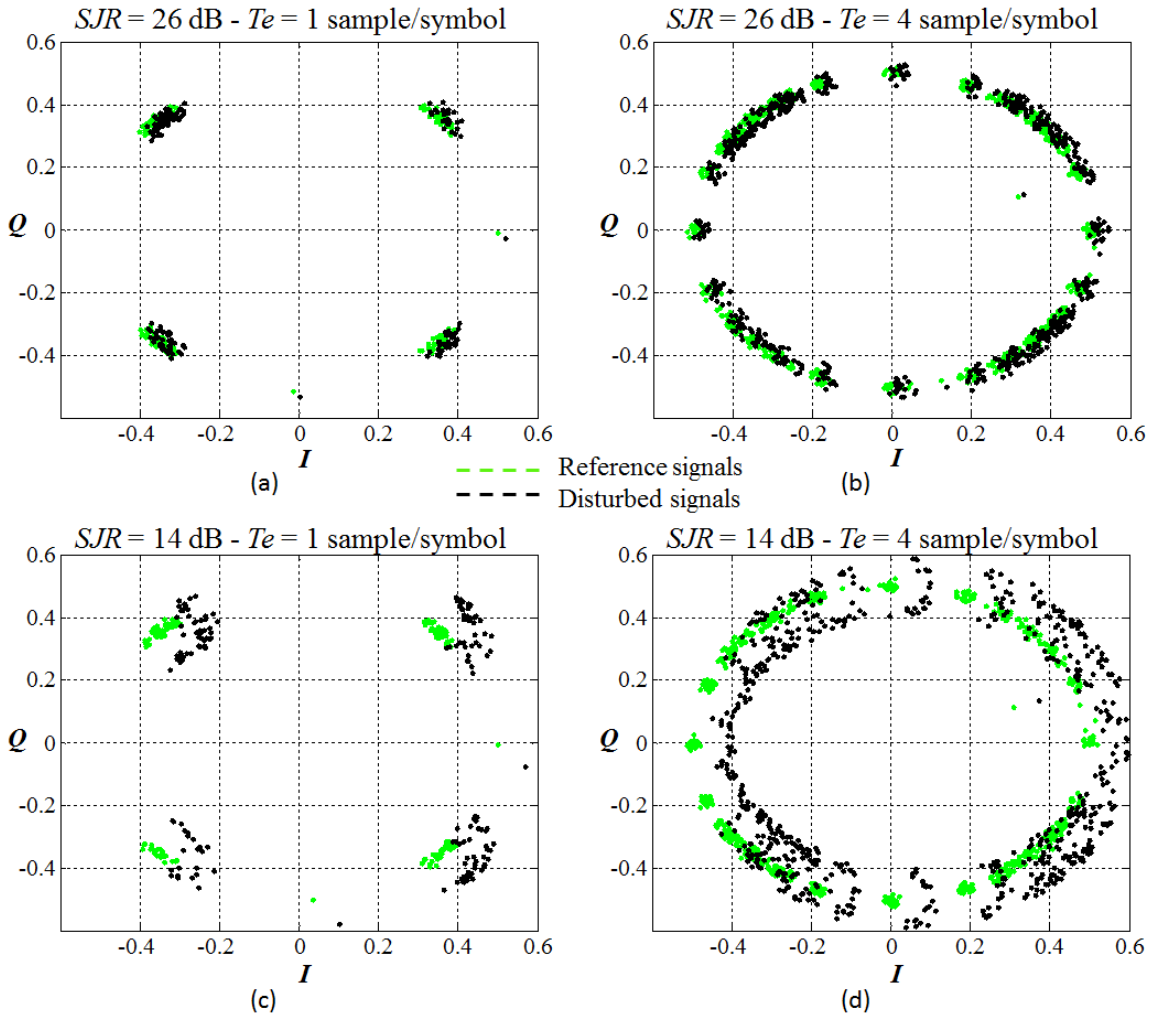


Figure 5 Constellations of I(nTe) and Q(enT) estimated in reception after passage in a AWGN channel of SNR = 30 dB and disrupted by a sinusoidal signal modulated around the GMSK carrier frequency for SJR = 26 dB (a, b) and SJR = 14 dB (c, d). The constellations are presented for two sampling values: T = 1 sample per symbol (a, c) and T = 4 samples per symbol (b, d). The reference signal is in green and disturbed signals are in red.

Taking into account the observed constellations, we defined two descriptors to characterize and discriminate the constellations corresponding to a normal environment and to a jammed situation. The descriptors are parameters calculated from the points of the constellation. Both descriptors are detailed in the following section.

4.3. Definition of the descriptors

4.3.1. Descriptor 1: radius of the points which composed the I/Q constellation

The first descriptor corresponds to the radius of the circle formed by $I(t)$ and $Q(t)$. It is defined by:

$$TT(t) = I^2(t) + Q^2(t) \quad (3)$$

The mean of this radius in normal conditions is constant - regardless of the sampling step.

As indicated above, the AWGN channel implies on the constellation a variance of TT(t) depending on the AWGN power. However, in Figure 4 and Figure 5, the variations on the radius are significantly increased by the presence of both jamming signals.

4.3.2. Descriptor 2: Error Vector Magnitude (EVM)

EVM is a parameter commonly used to assess the quality of modulation for communication systems.

This parameter gives an overview of the quality of the signal in addition of eye diagram or bit error rate (BER) measurements.

EVM indicates the difference between a reference constellation pattern of the constellation of estimated I/Q data. EVM is measured by computing the vector difference between the samples forming the reference constellation and the I/Q received samples. This is illustrated in Figure 6.

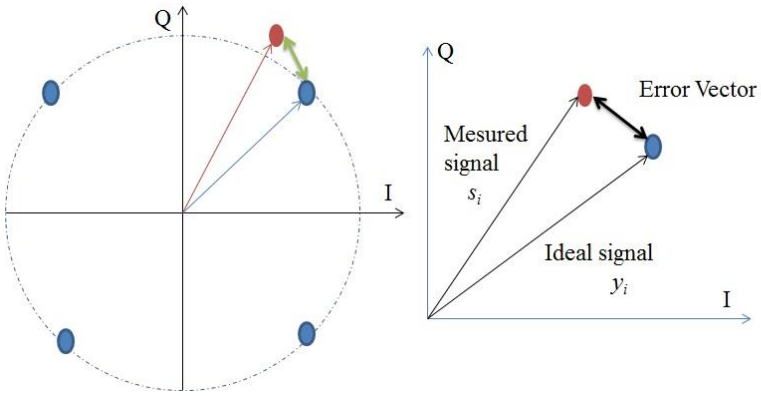


Figure 6 Constellation IQ and representation of EVM.

The expression of the *EVM* is given by:

$$EVM = |s_n - y_n| \text{ avec } \begin{cases} \|y_n\| = \sqrt{I_y^2(nT_e) + Q_y^2(nT_e)} \\ \|s_n\| = \sqrt{I_s^2(nT_e) + Q_s^2(nT_e)} \end{cases} \quad (4)$$

where y_n and s_n respectively represent the vectors defined by the components $I_y(_enT)$ and $Q_y(_enT)$ for the signal without jamming and by the components $I_s(_enT)$ and $_sQ(_enT)$ for the jammed signal.

Without jamming signal, EVM is depending on the variance produced by the AWGN channel. We define the EVM_{rms} as the mean EVM value over a time period equivalent to a burst duration. A burst is a train of symbols defined by the GSM-R communication standard, including 157 successive symbols.

$$EVM_{rms} = \sqrt{\frac{\sum_n |s_n - y_n|^2}{\sum_n |y_n|^2}} \quad (5)$$

EVM_{rms} indicates the state of the channel and can be estimated by the following relationship [2]:

$$EVM_{rms} \approx \sqrt{\frac{1}{SNR}} \quad (6)$$

This parameter provides a quantitative representation on the physical error introduced by the disturbances on the channel. Therefore, EVM_{rms} is a relevant descriptor to recognize the presence of an EM attack in relation to a normal functioning of the communication system (under assumption of *AWGN* channel).

4.4. Modelling of the 'normal' operating mode

For both descriptors, the modelling principle of the normal environment is identical. We recall that the normal environment corresponds to the absence of jamming signal.

For each descriptor, we determine a generative statistical model to represent the electromagnetic environment in normal state. The model is obtained from the different values taken by the $TT(t)$ or EVM_{rms} parameters, without jamming signal.

We make the assumption that for an *AWGN* communication channel, both parameters evolve according to a Gaussian law defined by a mean μ_x and a variance σ_x.

$$p_x(x) = \frac{1}{\sigma_x \sqrt{2\pi}} \exp\left(-\frac{1}{2} \left(\frac{x - \mu_x}{\sigma_x} \right)^2 \right) \quad (7)$$

For $x = TT(t)$, μ_x represents the mean value of the radius of the constellation and the variance is function of the variance of *AWGN*. For $x = EVM_{rms}$, the variance is also related to the variance of the noise of the channel.

For both descriptors, the mean and variance of the models are estimated based on maximum likelihood in using the following equations:

$$\mu_x = E[x] \approx \frac{1}{N} \sum_{n=1}^{N} x(n) \quad (8)$$

$$\sigma_x^2 = E[x^2] \approx \frac{1}{N} \sum_{n=1}^{N} x^2(n) \quad (9)$$

Figure 7 presents the histograms of the descriptor $TT(t)$ of the I/Q estimated constellation for different situations:

- in presence of only an AWGN channel,
- in presence of an AWGN channel + a jamming pure sine signal centred on the frequency channel of the GMSK communication ($G_1(t)$) (figures 7(a) and 7(b)) and,
- in presence of an AWGN channel + a jamming sine signal modulated around the frequency of the GMSK communication ($G_2(t)$) (figures 7(c) and 7(d)).

The histograms are computed using data obtained using a dedicated laboratory measurement testbed. For each jamming signal, the results are given for two different *SJR*.

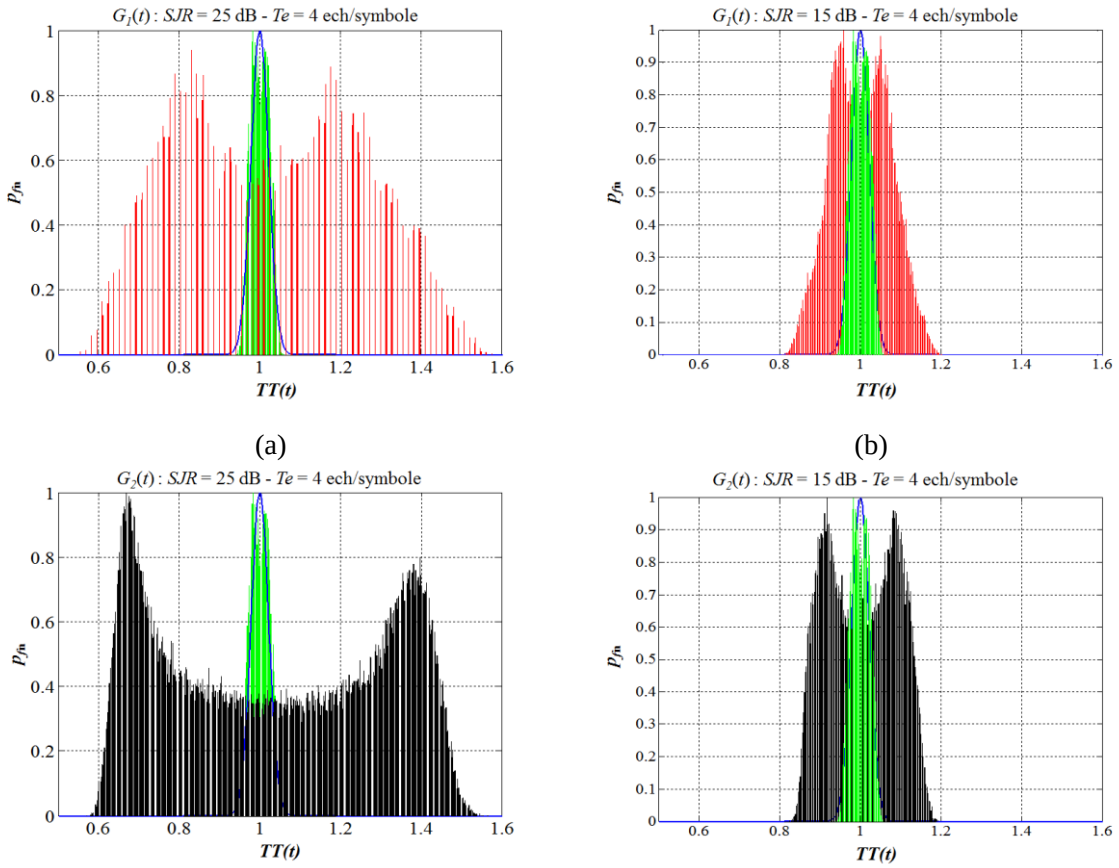


Figure 7. The green histogram corresponds to TT(t) distribution for 'normal' conditions, i.e. for an AWGN channel with an SNR = 30 dB. The red TT(t) histograms are obtained in presence of a jamming pure sine signal, for a SJR= 25 dB (a) and SJR = 15 dB(b). Black TT(t) histograms corresponds to signals disturbed by a jamming sine signal modulated around the GMSK carrier frequency, for SJR= 25 dB : (c) and SJR = 15 dB (d).

In this figure, we observe that the histograms for both jammed signals are shifted as a function of the SJR value.

For G1(t), we obtain that the histograms are more widely spread and shifted for the considered SJR value of 25 dB.

For G2(t), which represent a more aggressive perturbation, this shift is already becoming quite distinct for low values of SJR, starting at 40 dB.

This is also the reason why we consider in this second section of histograms the two 40 dB and 25 dB SJR values.

Figure 8 now presents the histograms of the descriptor EVM_{rms} for the normal and jamming conditions described previously.

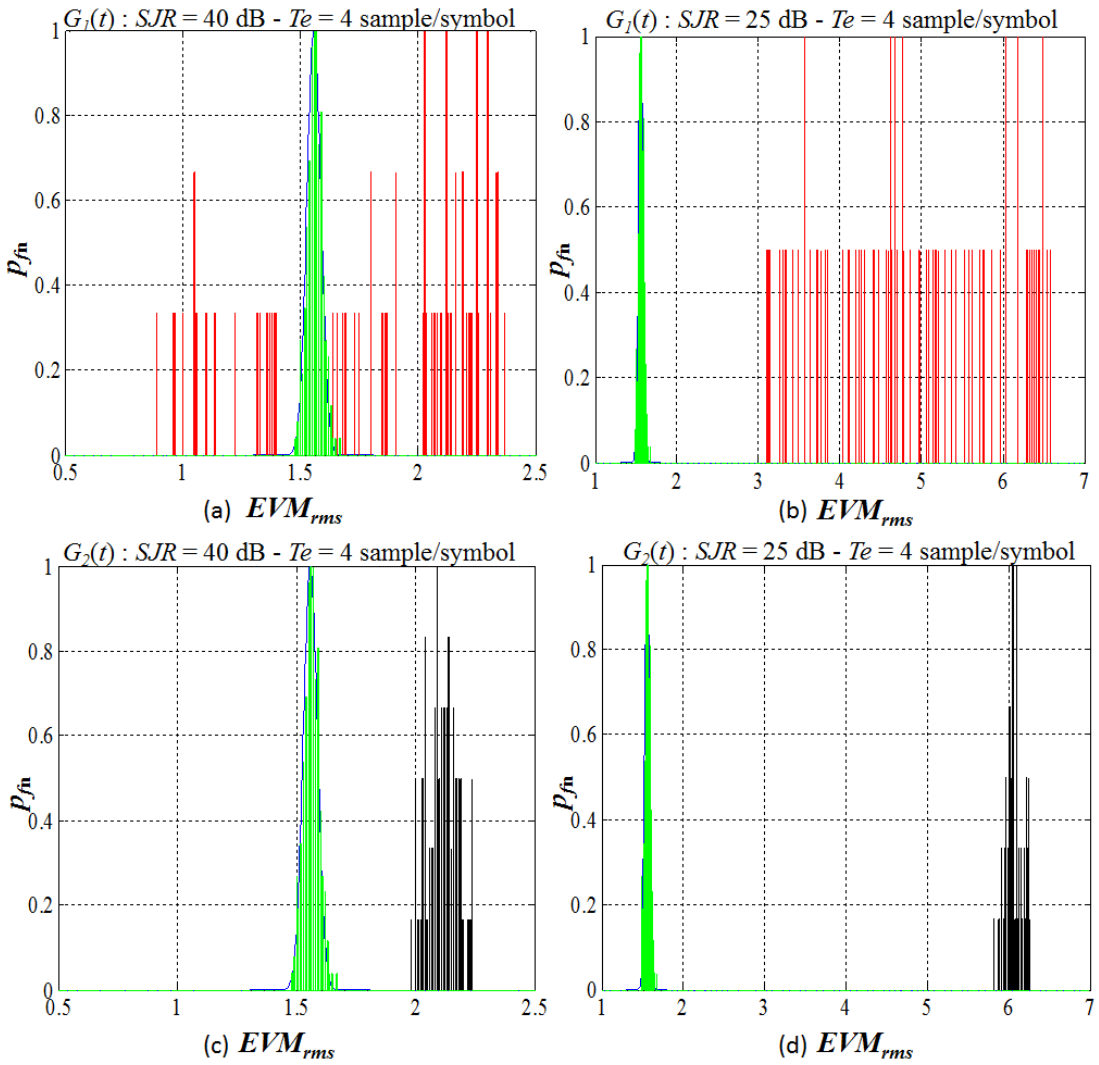


Figure 8. The green histogram corresponds to EVM_{rm} distribution for 'normal' conditions, i.e. for an AWGN channel with an SNR = 30 dB. Red EVM_{rms} histograms correspond to signals disrupted with a sinusoidal signal for SJR = 40 dB (a) and SJR = 25 dB (b). Black match histograms of the EVM_{rms} for signals disturbed with an sine-modulated signal around the GMSK carrier frequency for SJR = 40 dB(c) and SJR = 25 dB. (d)

We conclude that we obtain more distinguishable and consequently more easily used results using EVM_{rms}.

4.5. EM attack detection

Looking at the modification of the distribution of the descriptors in presence of jamming signals, we propose to carry out a supervised EM attack detection.

We preliminary constituted a data base corresponding to the normal environment. The data base is composed of measurements performed in different situations in absence of jamming signal. From this data base, reference distributions of the descriptors were obtained. That step corresponds to the learning phase. The distribution of the data in normal operation is described by a Gaussian distribution. This permits to simplify the detection. Indeed, the Gaussian distribution is symmetrical defined by an interval around the mean of the distribution. The interval is defined by the minimal and the maximal values of the Gaussian which car be expressed as a function of the variance.

$$x_{MAX} \approx \mu_x + 3\sigma_x \quad (10)$$

$$x_{MIN} \approx \mu_x - 3\sigma_x \quad (11)$$

Once these models learned,, the detection consists in comparing the descriptors measured to the threshold defined by the minimal and maximal value of the normal distribution descriptors the min and

max considering Gaussian model detection will follow the following expression:

Then, the method consists in comparing the descriptor observed to threshold values defined x_{min} and x_{max}.

$$\text{If } x \in [x_{MIN}, x_{MAX}] \quad \text{then normal operation;}$$
$$\text{Otherwise } EM \text{ attack detection} \tag{12}$$

4.6. Results

We present different results of detection using these two parameters in real environment along the railway tracks. We describe the measures carried out and the obtained results.

4.6.1. Description of the measurement configuration

We carried out measurement along the tracks of a HST line where the GSM-R is not yet deployed in order to avoid to disturb the railway communications. Figure 9 presents the measurement configuration.

A GMSK frame was generated using a horn antenna and the signal received by a GSM-R antenna was measured. A GSM jammer was activated on demand to jam the GSMK signal.

Figure 9. Measurements along the railway tracks at Mory (F)

A GMSK generator from Rohde & Schwarz was employed to generate a 4 dBm power signal at the output of the generator. By activating the jammer and associating different attenuators at its output, the detection was tested for different SJR (between 3 dB and 23 dB), measured at the output of the GSM-R receiving antenna. The FSIQ7 demodulator was connected to the GSM-R antenna as illustrated in Figure 10 to collect the I/Q representation.

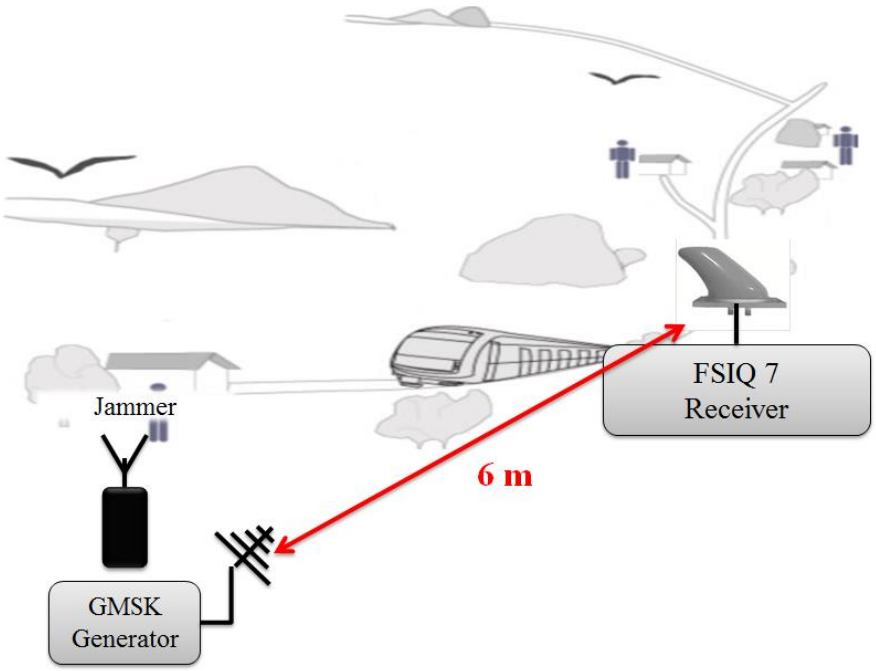


Figure 10. Measurement in the quadratic space

150 bursts were employed for the learning phase, containing only the data resulting of the signal of communication and the EM noise of the railway site. Regarding the sampling rate, 88 800 samples of radius *TT*(*t*) were employed for the learning phase.

The detection process was tested over a data base of 1200 measured bursts. Behind these 1200 measured bursts, 330 bursts were measured in normal operation and 870 bursts were measured while activating the jammer. The data base of 1200 measured bursts then corresponds to 1200 EVM_{rms} and to 515 040 samples of radius *TT*(*t*).

4.6.2. Results of the detection with the EVM_{rms} descriptor

Figure 11 presents the evolution of the EVM_{rms} measured in railway site when we successively switch on and switch off the jammer.

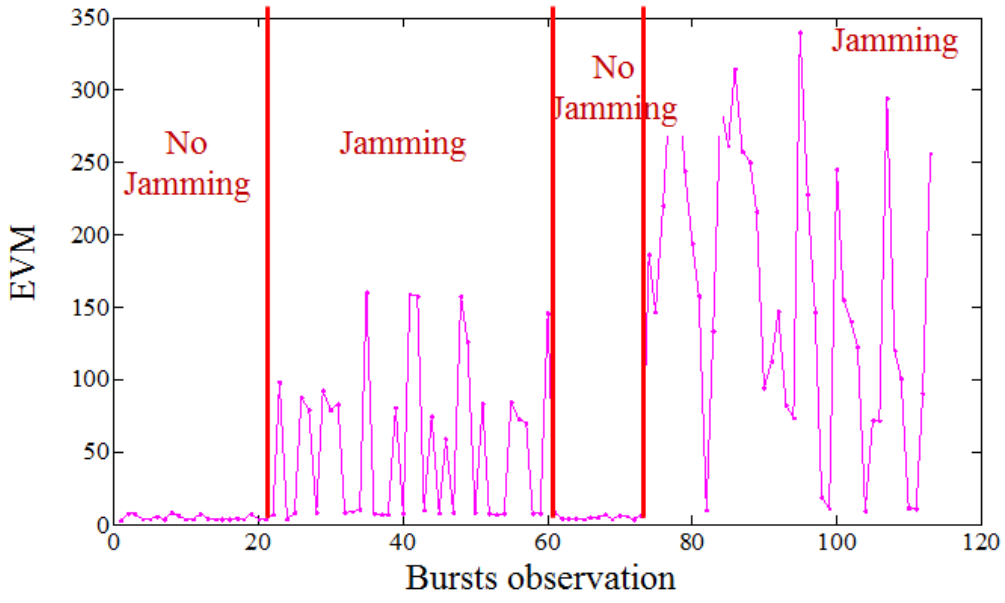


Figure 11. Observation of bursts with and without jamming.

- **Processing on a burst**

We present in the following table the percentage of good detection over 870 bursts measured in the jammed mode and the percentage of false detection over 330 bursts measured in normal operation.

Table 1. Detection rate of disturbance on 1 burst.

Mode	Detection	Loss detection
Disturbed	85.73 %	14.27 %
Mode	**Detection**	**False alarms**
Non disturbed	97.56 %	2.45 %

The detection rate is not perfect and we observed 2.45 % of false alarms. To understand the origin of these false alarms, Figure 13 presents the 330 EVM_{rms} values obtained without jamming. In this figure, the horizontal line corresponds to the threshold of detection and we notice that certain EVM values exceed this threshold.

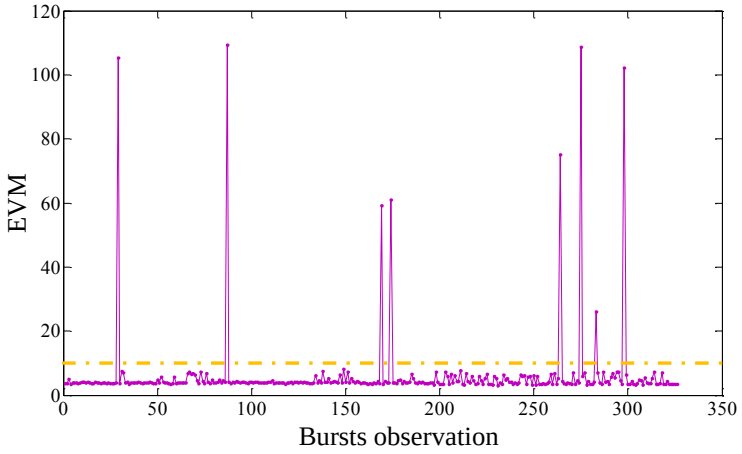
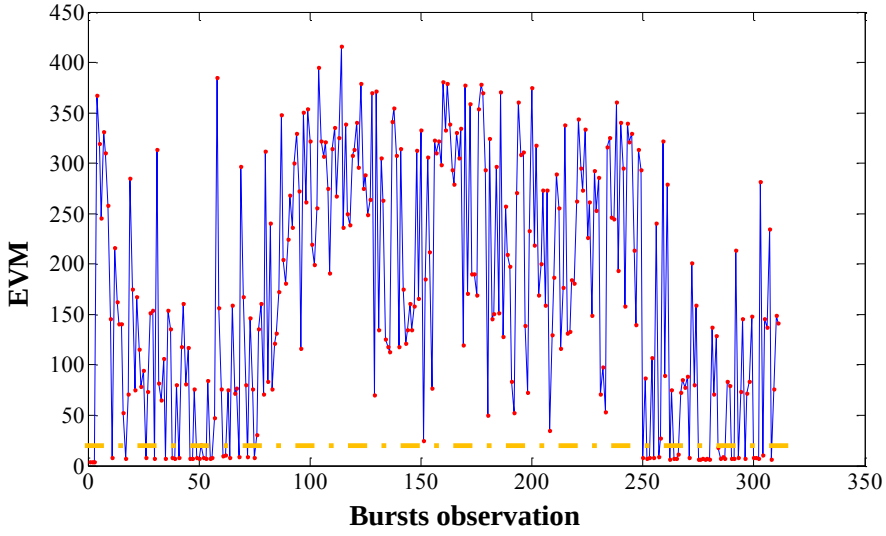


Figure 12. Observations of EVM without jamming.

These important variations of the EVM generate the false alarms. They mainly come from the transient disturbances present in the railway environment.

Figure 13 presents EVM_{rms} values obtained in presence of jamming. In this figure, the horizontal line corresponds to the threshold of detection.



(b)

Figure 13. Observations of EVM with jamming.

We observed that certain EVM values are lower to the detection threshold. This explains the 14.27% of missed detection.

Knowing that, in absence of jamming, the EVM values which exceed the threshold are very erratic, we then try to consider several successive EVM values in order to improve the overall performance.

- **Multi-burst processing**

In order to minimize these false alarms and to improve the detection rate, we consider a longer period of detection corresponding to a selected 8 bursts duration. This duration corresponds to the duration of a GSM-R frame (8 time slots, the slot represents a burst). We analyse the percentage of EVM values lower and greater to the threshold over this 8 bursts period.

Figure 14 presents the percentage of values superior to the threshold for the data collected in normal situation and for the data collected in jammed situation.

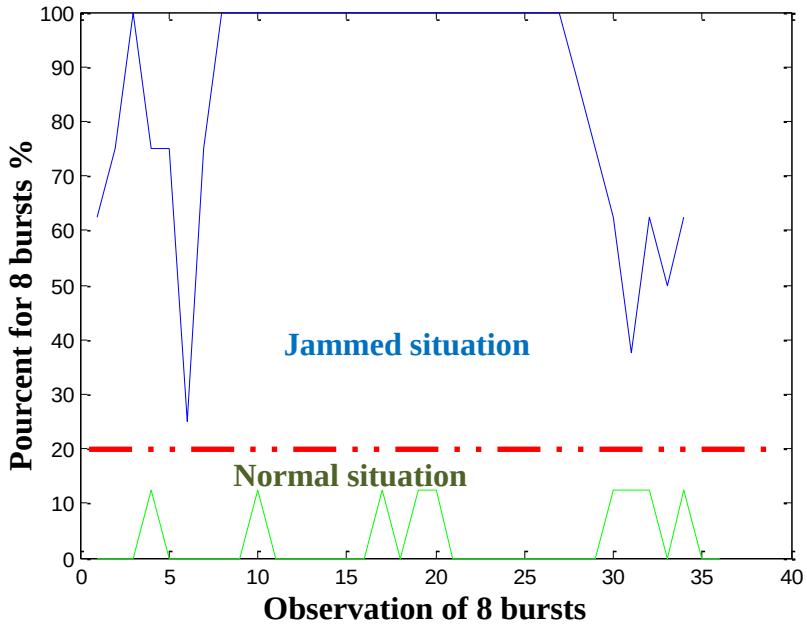


Figure 14. Detection rate during 8 consecutive bursts with and without jamming.

We observe that during these 8 bursts, more than 25 % of the values are over the threshold for the data in presence of jamming, while a maximum of 15 % of data obtained in normal situation exceeds the threshold.

We then define a new threshold defined by the percentage of data exceeding the threshold. The threshold value was fixed as 20%. This new method improves the detection and provides perfect results, as shown on table 2. It also avoids the false alarms.

Table 2. Detection rate on 8 bursts

Mode	Detection	Loss detection
jammed	100 %	0 %
Mode	Detection	False alarms
Non jammed	100 %	0 %

4.6.3. Results of the detection with the TT(t) descriptor

We assess the relevance of this second descriptor using the same database than for the EVM.

- **Processing on a burst**

In Table 3, we present the percentage of good detection obtained behind the data collected in jammed mode and the percentage of false detection obtained behind the data measured in normal operation.

Table 3 Detection rate on one burst with TT(t)

Mode	Detection	Loss detection
Jamming	97.56 %	2.44 %
Mode	Detection	False alarms
Non jamming	76.20 %	23.80 %

Once again, the detection is acceptable but is not optimal and we notice a high percentage of False Alarms. In consequence, we need to improve the detection system. This time also, we extend the duration of observations.

- **Processing on symbols**

In this step, we adapt the model to simultaneously improve the detection and avoid false alarms.

We progressively extend the period of observation up to obtain an efficient detection and we analysed the percentage of TT value exceeding the threshold for the jammed and the normal situation.

Considering 5 successive bursts, we distinguish the percentages corresponding to both situations. Table 16 provides the representation of the percentage of TT value exceeding the threshold over a 5 successive bursts period. We observe that for jammed situations, more than 25 % of the value are upper the threshold whereas a maximum of 20 % of the values exceeds the threshold without jamming. By defining an intermediate percentage, we are able to distinguish between the two situations providing 100 % of good detection and avoiding false alarms.

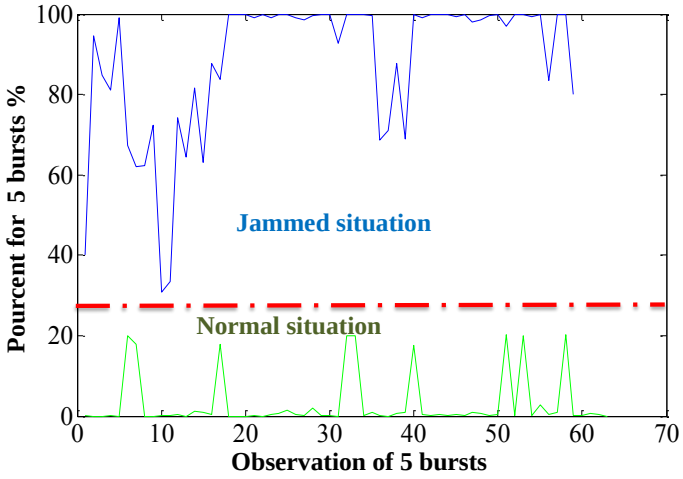


Figure 15. Detection rate during 5 bursts successently with and without jamming.

If more than 25 % of the value are upper than the threshold so we are in jammed situation. In the other case we are in normal situation. Using this new reasoning we can obtain 100 % of good detection and avoid all the false alarms, as shown on table 4.

Table 4. Detection rate over an extended 5 bursts period

Mode	Detection	Loss detection
Jamming	100 %	0 %
Mode	Detection	False alarms
Non jamming	100 %	0 %

4.7. Conclusion

This first approach and its associated descriptors demonstrate a real potential detecting jamming situations by using the I/Q information. This approach does not need any supplementary equipment since it uses the IQ information extracted from the used receiver itself. This can be considered as an advantage since it limits the additional cost of the detection equipment. However, this could be also considered as a drawback since, currently, the IQ data, although existing in the receiver is not available through an external receiver port. Therefore, a new generation of equipment can be necessary with this additional new port or integrating the detection algorithm in the receiver processing unit.

Moreover, if an EM attack can be detected using this approach, the recognition of the used jammer is not possible. Using a second approach, now presented in the second part of the deliverable, a simultaneous EM attack detection and jammer recognition approach could be developed. The detection method will be thoroughly examined.

5. Detection of attacks in spectral space

This section describes the second approach for the detection of jamming signals which was studied in this task. This approach is based on the statistical analysis of the locally received spectrum.

5.1. Railway critical environments to be considered

In a first step, to evaluate normal electromagnetic conditions (without jamming), it was decided to perform electromagnetic environment measurements in different railway representative environments.

5.1.1. Railway line

To obtain a general understanding of a normal railway electromagnetic environment, electromagnetic environment measurements were carried out along a representative railway line where low or medium power jammers could be positioned discreetly. One possible objective could be to jam the ground to train communication based on GSM-R. The measurements were recorded in the vicinity of Chateau-Thierry (F), along the LGV East line (cf. D3.1), without jamming, in order to statistically analyze the distribution of the spectrum in normal conditions, along the track.

5.1.2. Station

It was also decided to measure the electromagnetic environment conditions in railway stations that are strategic places where electromagnetic attacks could occur. Two railway stations were selected to be representative for the study: the Paris Gare de l'Est railway station and the Liège Gare des Guillemins railway station. Measurements in Paris Gare de l'Est were performed in three different measurement locations: along the platform, in front of the control command centre of the station, and at Level -1, below the platforms of the station at the junction between the railway and the subway stations. In the Liège Gare des Guillemins railway station, measurements were performed at the platform level (see deliverable D3.1).

5.1.1. Train

Finally, measurements were also performed in a TGV SNCF test train, named IRIS, during a high speed trip between Paris and Strasbourg.

5.1.2. Results of in situ measurement campaigns

Deliverable D3.1 presents these results and an initial analysis of the measurement campaigns that we propose to briefly recall here. Measurements in the GSM-R band were performed with a span setting of 100 MHz and a central frequency of 925 MHz. A span setting of 10 MHz, at a central frequency of 923 MHz, i.e. in the middle of the GSM-R downlink band, was also used.

Concerning the measurements performed along the LGV East line, signals coming from GSM-R Base Transceiver Stations (BTS) installed along the LGV line are easily visible in the GSM-R downlink frequency band. We notice signals coming from several GSM-R BTS installed along the LGV line. In general, at each measuring place, we observe two different GSM-R BTS signals received at different power levels. Along the line, the measuring location is situated between two consecutive BTS. Therefore, in general, these signals correspond to the closest BTS, for the strongest received signal and, to the farthest BTS, for the lower power signal. As the trains are circulating along the line, handovers occur in order to maintain the communication while the train passes in front of the consecutive BTS of the fixed terrestrial network. As a consequence, at any place along the railway line, a limited number of GSM-R BTS signals must be detected operating at different frequencies. In Paris Gare de l'Est and in Liège Guillemins the observations are the same since received signals are quite strong, corresponding to good radio coverage from local BTS.

Below the GSM-R allocated downlink frequency band, no radio communication activity is discernible on our measuring sites. In a frequency band right over the GSM-R allocated frequencies, we observe

the telecom operators GSM downlink band activity. In stations Paris Gare de l'Est and Liège Guillemins Gare, numerous strong signals are received in this band, corresponding to a large cellular phone activity, normal in these urban environments.

In the uplink GSM-R frequency band, from 876 to 880 MHz, GSM-R is in use for train to ground voice communications, but not yet for ERTMS Level 2 signalling. To the contrary of signalling, voice communications are not used 100 % of time. As a consequence, a rather low radiocommunication activity was measured on the uplink on all our measurement sites. Therefore, signals were captured very rarely.

Below the GSM-R uplink band, no activity is visible. Above the GSM-R uplink band, we observe the GSM uplink band with few signals coming from cellular phones. In stations, this band is fairly busy due to the number of potential cellular phone users in the station and its surroundings.

Moreover, we observed that, for a same location, the mean and the standard deviation of the measured spectrum are relatively stable. However, we detected variations of the spectral means and of their standard deviations due to the presence of very different signal to noise ratios. These variations are mainly due to the variability of the characteristics of communication signals or, basically, by the presence or absence of communication. Finally, if we consider the observations as a function of the location, we observed different comportments of the EM environment.

Starting from these preliminary observations, the following section develops the analysis performed using these various EM environment measurements. These results will allow us defining the parameters and models most suitable for an automatic detection system of EM attacks.

5.2. Analysis of the EM environment

5.2.1. Introduction and context

We keep in mind that the initial goal of this task is to analyze and characterize the EM environment in 'normal' conditions, using the spectral observations performed between 875 MHz and 975 MHz (span setting of 100 MHz, centred at 925 MHz) composed of 500 p.s.d. values with a sampling step of 0.2 MHz.

5.2.2. Analysis and characterization of the EM environment in normal conditions

In order to better understand the EM environment in 'normal' conditions, we realized a study that consists in estimating the distribution of measured p.s.d. by estimation of histograms.

We carried out these estimations according to the measurement sites (in Paris Gare de l'Est, Liège Guillemins, LGV East line and in the high speed test IRIS train) and also according to the communication frequency bandwidth (uplink and downlink GSM-R, GSM and the rest of observed frequency band). This analysis will allow determining the adequate statistic model and the best definition of associated parameters.

5.2.2.1. Analysis of distributions of p.s.d. according to the measurements sites and the frequency bandwidths

Figure 17, Figure 18 and Figure 19 present the estimated histograms. They respectively correspond to the collected data along the LGV East line, at the station Paris Gare de L'Est, at the Station Liège Guillemins and in the IRIS train. For each figure, the spectral observations are presented (subfigures (b)). The subfigures (a) present, the estimated histogram of p.s.d. values S(f) for f from 875 MHz to 975 MHz. The subfigures (c) present, the estimated histograms of p.s.d. values S(f) for the five following frequencies bandwidths :

- The group of bandwidths out of communication bandwidths: 875-876 MHz, 916-921 MHz and 961-975 MHz. We label this various bandwidths 'other band'.

- The uplink GSM-R bandwidth : 876 - 880 MHz
- The uplink GSM bandwidth: 880 - 915 MHz
- The downlink GSM-R bandwidth: 921 - 925 MHz
- The downlink GSM bandwidth: 925 - 960 MHz

Firstly, we consider Figure 16, relative to the spectrum of EM environment measured along the LGV East line. These data are composed of 30929 spectrums. Between 875 MHz and 975 MHz, the complexity of the spectrum distribution is due to the exploitation or not of the frequency channels by communication systems. In Figure 16(a), we observe a principal mode at a -100 dBm power level. It corresponds to the EM noise environment that can be found in the non-used channels. As indicated previously, this is particularly the case of the uplink bandwidths of GSM-R and GSM and of some channels of the GSM-R downlink not used at the different measurement locations.

However, Figure 16(c) shows that this mode is strongly composed of the channels not reserved to the communication systems and of the GSM uplink. Finally, on Figure 16(a), the histogram presents three another weaker modes corresponding to -85 dBm, -69 dBm, and -52 dBm power levels. As we can see on Figure 16(c), these modes are mainly generated by the presence of many GSM BTS close the measuring locations.

Observing Figure 16(c), we obtain that the repartition of p.s.d. follows the repartition of p.s.d. values of the GSM bandwidths. The uplink and GSM downlink represent 70% of the observed bandwidth. More precisely, we can note that the histogram of the p.s.d. of the GSM uplink bandwidth present one mode at -100 dBm that it is not centred; no or very few radiocommunication activity is present in this bandwidth. Histogram of the GSM downlink is more complex. It presents four modes: the first around -97 dBm represents the channels with weak energy emitted from distant BTS. Very few channels without signal are present in this bandwidth and are not really visible in this histogram. The three other modes are the modes introduced while analyzing Figure 16(a).

The p.s.d distribution shape of the GSM-R uplink bandwidth is the same than the p.s.d. of the GSM uplink. Without activities, it presents one mode at a -100 dBm power level and it is also no centred.

Concerning the GSM-R downlink, this conclusion is no more valid, the corresponding histogram is characterized by three relatively emphasized modes. The limited number of ‘visible’ GSM-R BTS signals from the same location measurement mostly determines these results. Indeed, a large number of the allocated GSM-R channels are not used. This has for consequence the first mode at a -100 dBm power level which is the local noise floor. The two other modes are linked to the two close GSM-R BTS received signals.

From these histograms, many conclusions can be drawn to guide the EM model estimation.

As a function of the bandwidth, the obtained p.s.d. correspond to different distributions. In consequence, it is preferable to build a model for p.s.d. for each channel (or covering a limited bandwidth) instead of using only one model representing simultaneously all the frequency channels. Indeed, if we cover a wide frequency band at a time then, we lose most of the information related to the ‘normal’ absence of signals in the spectrum. Moreover, as a function of the studied frequency bandwidth, the model will be more or less complex, containing one or many modes. If only one mode is present, the distributions are not centered. Thus, even in this case, without specific processing of the p.s.d., the model is not a simple distribution like a Gaussian distribution.

Figure 17 relative to the measurements in Paris Gare de L’Est, we almost obtain the same histogram shapes that in Figure 16. However, some non negligible differences appear. One main difference is the position of the stronger mode of the histograms at -90 dBm. The EM noise environment is stronger by a factor of 10 dB to the EM noise measured along the LGV East line. This is explained by the strong local electromagnetic activity found in urban environments as compared to the rural environment. The second is the relative flatness of the histograms between -70 dBm and -35 dBm. The stronger local GSM and GSM-R BTS levels of activity and the multipath propagation effects decrease the mode accentuation in the GSM and GSM-R downlink bandwidth.

The same conclusion is also drawn from Figure 18 concerning the measurements performed in Liège Guillemins station. Although the stronger mode is still located at -100 dBm, like for the measurements performed along the LGV East Line, the histograms present equally flatness shapes but still different of the ones obtained in Gare de l’Est station.

In consequence, the EM environment localization involves various differences on the p.s.d. distribution for every frequency channels. Either the histogram shape is different (GSM and GSM-R downlink), or the mode location can be different in the case of 'simple' distribution (case of the p.s.d. of bandwidths without signal being enable equal to -90 dBm or -100 dBm). In consequence, the model estimation should be different in function of the location.

We conclude this preliminary analysis by presenting Figure 19. These measurements were obtained aboard the IRIS high speed train vehicle in movement along the LGV East line. This non-stationarity of the measuring location has a direct impact of the distribution of the p.s.d. Indeed, signal levels observed from the (GSM or GSM-R) BTS quickly evolve according to the vehicle movement. As complementary information, during the measurements, the IRIS high speed train crosses a GSM-R cell, from one BTS to the following BTS in a minute or so. Consequently, multipath effects are also evolving rapidly. The consequence is a distribution with an upper part almost monotone from -70 dBm to -35 dBm. Of course, the only shared characteristics are the absence of signal in uplink bandwidths of communication and in the bandwidths not used by the communication systems.

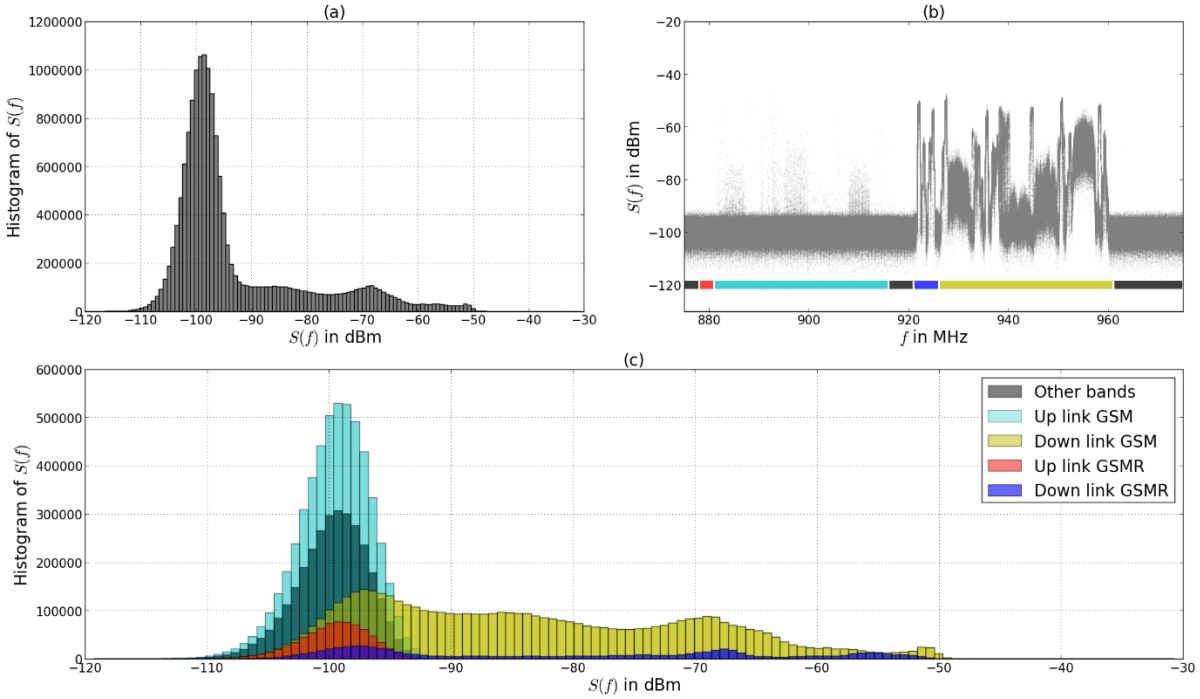


Figure 16. Histograms of 30929 spectral measurements performed along the LGV East line (a): Histogram of 30929 x 500 spectral components S(f). (b) The 30929 spectral measurements form f = 875 MHz to f = 975 MHz (c): Histogram of 30929 spectral components S(f) in function of the spectral bandwidth. One color represents one communication spectral bandwidth as indicated in the legend.

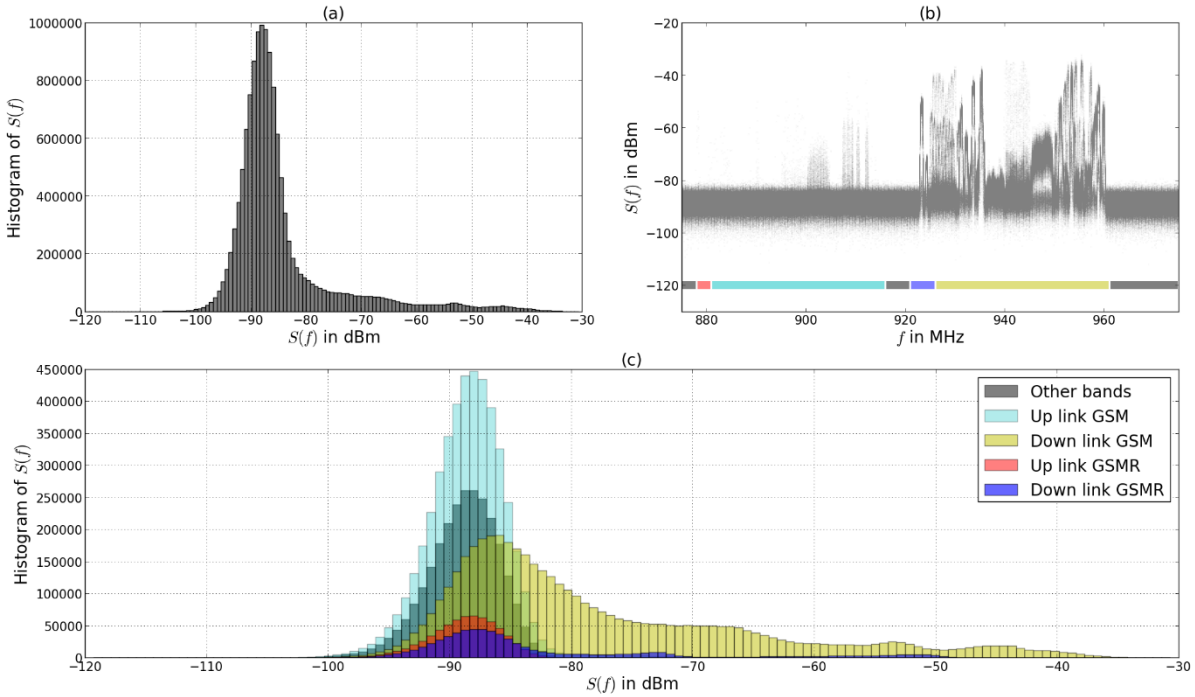


Figure 17 : Histograms of 26165 spectral measurements performed at Paris Gare de l'Est. (a) : Histogram of 26165 x 500 spectral components S(f). (b) The 26165 spectral measurements form f = 875 MHz to f = 975 MHz (c): Histogram of 26165 spectral components S(f) in function of the spectral bandwidth. One color represents one communication spectral bandwidth as indicated in the legend.

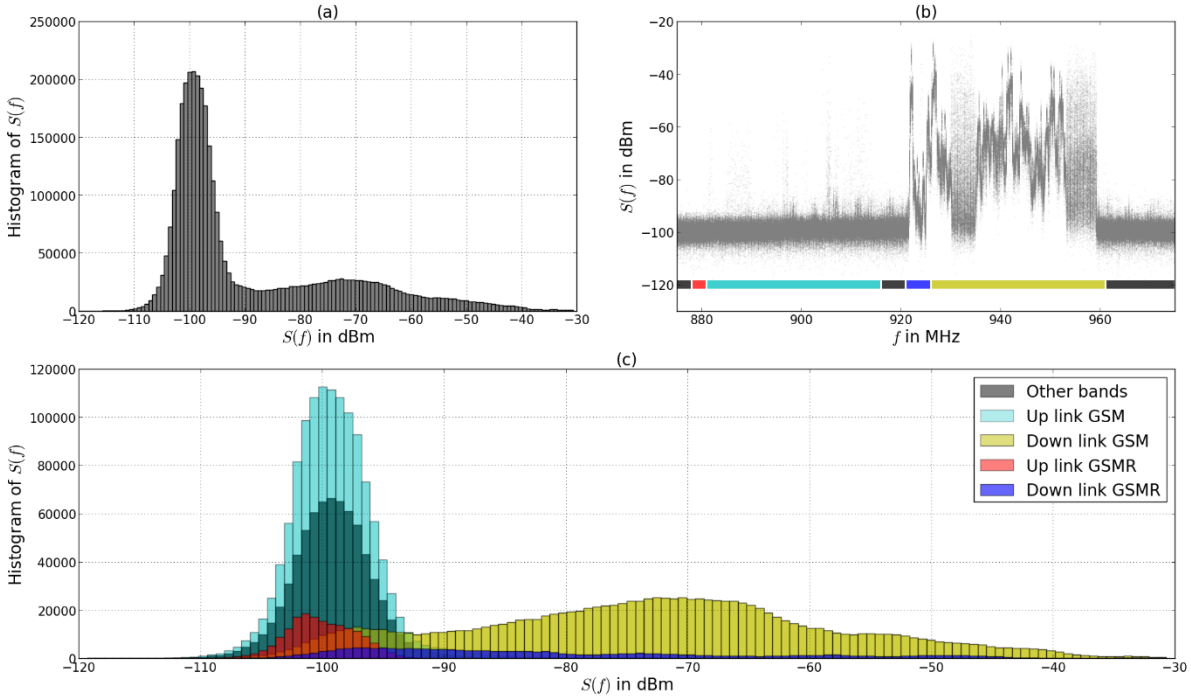


Figure 18. Histograms of 7157 spectral measurements performed at Liège Guillemins. (a): Histogram of 7157 x 500 spectral components S(f). (b) The 7157 spectral measurements form f = 875 MHz to f = 975 MHz (c): Histogram of 7157 spectral components S(f) in function of the spectral bandwidth. One color represents one communication spectral bandwidth as indicated in the legend.

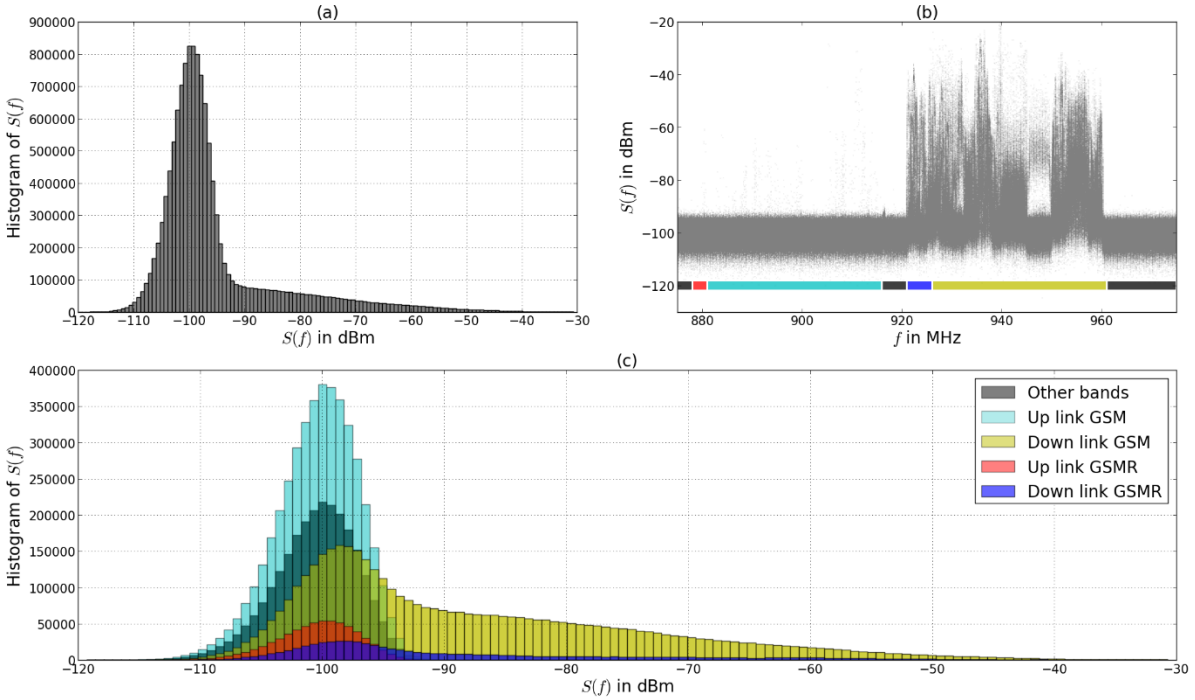


Figure 19 Histograms of 25210 spectral measurements performed aboard the IRIS train. (a): histogram of 25210 x 500 spectral components S(f). (b) The 25210 spectral measurements form f = 875 MHz to f = 975 MHz (c): Histogram of 25210 spectral components S(f) in function of the spectral bandwidth. One color represents one communication spectral bandwidth as indicated in the legend.

5.2.2.2. Analysis of distributions of p.s.d. according to the frequency channels

The precedent subsection presented the histograms of the p.s.d. considering the various measurement sites and the various frequency bandwidths explored. This allowed highlighting the differences between our selected different environments and considered bandwidths.

We conclude by considering more effective to develop different specific p.s.d models rather than one model covering all frequencies.

We now present an analysis of p.s.d considering the distribution of two consecutive frequencies observed in three contexts.

The first set concerns two p.s.d. S(f) observed at f = 876 MHz and f = 876.2 MHz in the GSM-R uplink frequency bandwidth. The second set corresponds to f = 922 MHz and f = 922.2 MHz in the GSM-R downlink bandwidth. Finally, the last set is chosen in the GSM downlink bandwidth at the frequency f = 944.6 MHz and f = 944.8 MHz. The results are respectively presented in Figure 20, Figure 21 and Figure 22. For each figure, the subfigures (a) and (b) represent the histogram of both selected p.s.d. The subfigures (d) and (e) present their evolution as a function the acquisition. Finally, the subfigure (b) presents the joint distribution of these frequency channels: S(f+0.2 MHz) = fct(S(f)). The measurement site is the LGV East line.

We start analyzing these results by considering Figure 20. In the GSM-R uplink bandwidth, the presence of communication signal is very occasional. The histograms of both p.s.d. are characterized by one mode at -100 dBm. Even considering only frequency channel, the histograms are not centred (cf. Figure 20(a) Figure 20(e)). This dissymmetry increases if we observe the distribution presented Figure 20(b). The higher values are more concentrated than the lower values. This is probably due to the overall dynamic of the measuring equipment in conjunction with its noise floor. On this same subfigure we can see a correlation between these two consecutive frequencies Figure 20(b).

In Figure 21, the histograms present many modes. The selected frequency channels are in the GSM-

R downlink frequency band. Moreover, we have chosen the first frequency at the peak of the lobe signal from a GSM-R BTS. On these figures, it appears two modes, one mode is around -54 dBm and a second one, very weak, is at -100 dBm. After a more thorough analysis, we have concluded that these points are not realistic and are artefacts generated during the acquisition step. The second consecutive frequencies have the same characteristic that the previous frequencies with a large variance around the mode situated at -60 dBm. Once again, the second mode is not considered realistic (Figure 21(e)).

Concerning the frequencies in the GSM downlink bandwidth (Figure 22), we observe many modes on the histograms of both p.s.d. The first mode, at -100 dBm, corresponds to realistic points and results of the communication principle used in the GSM communication system. Indeed, radiofrequency transmission is not always performed on the same physical channel but, using frequency hopping, exploits different frequency channels. The other modes are complex and are probably due mainly to the multipath effect of the EM environment, at this particular location.

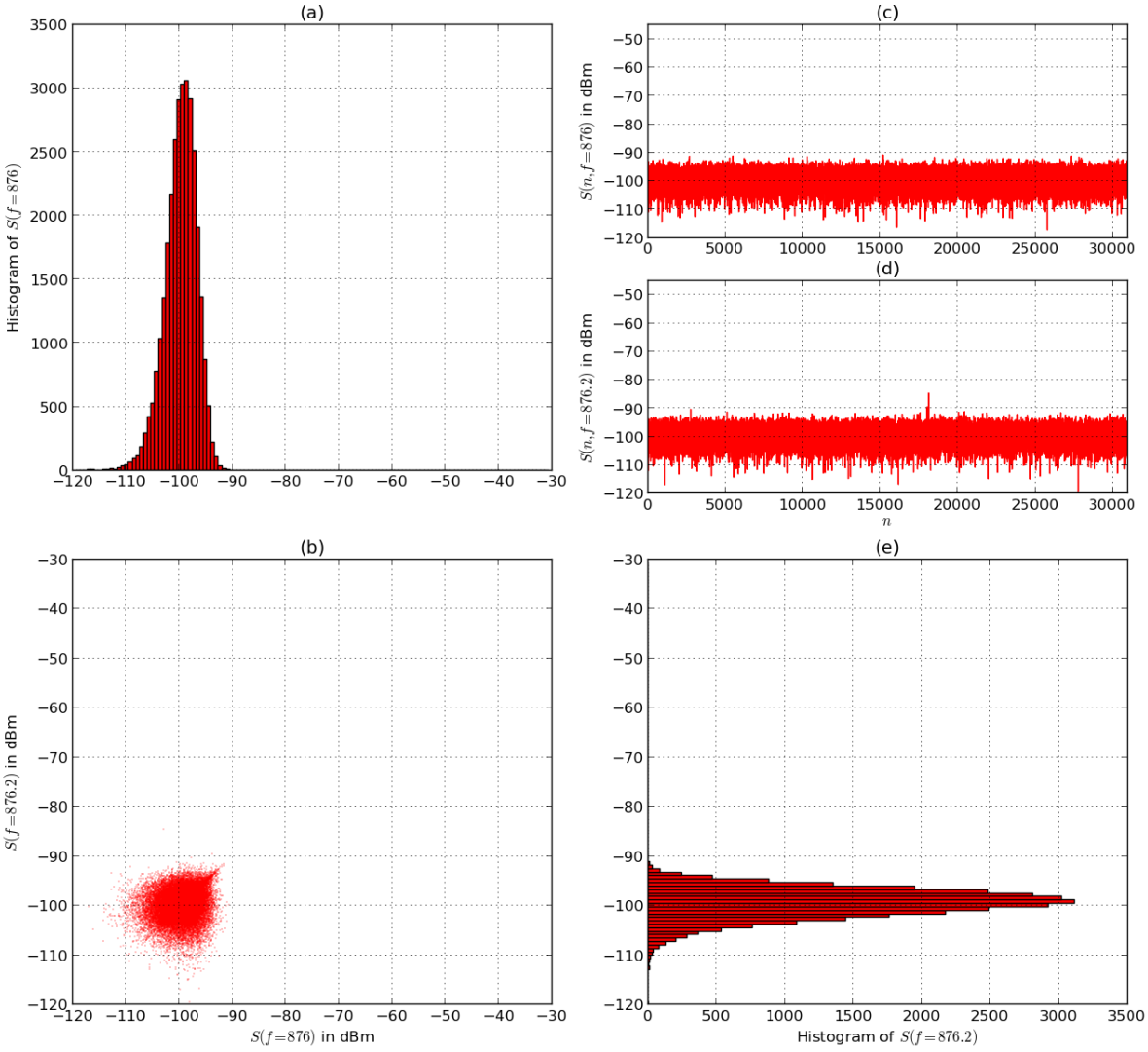


Figure 20 Analysis of two adjacent spectral components in the GSM-R uplink bandwidth for the measurements performed along the LGV East line. (a) and (e) are respectively the histograms of 30929 values of S(f) at f = 876 MHz and at f = 876.2 MHz. (c) and (d) are respectively the 30929 consecutives values of S(f) at f = 876 MHz and at f = 876.2 MHz. (b) is the representation of the joint distribution of S(f) at f = 876 MHz as a function of S(f) at f = 876.2 MHz.

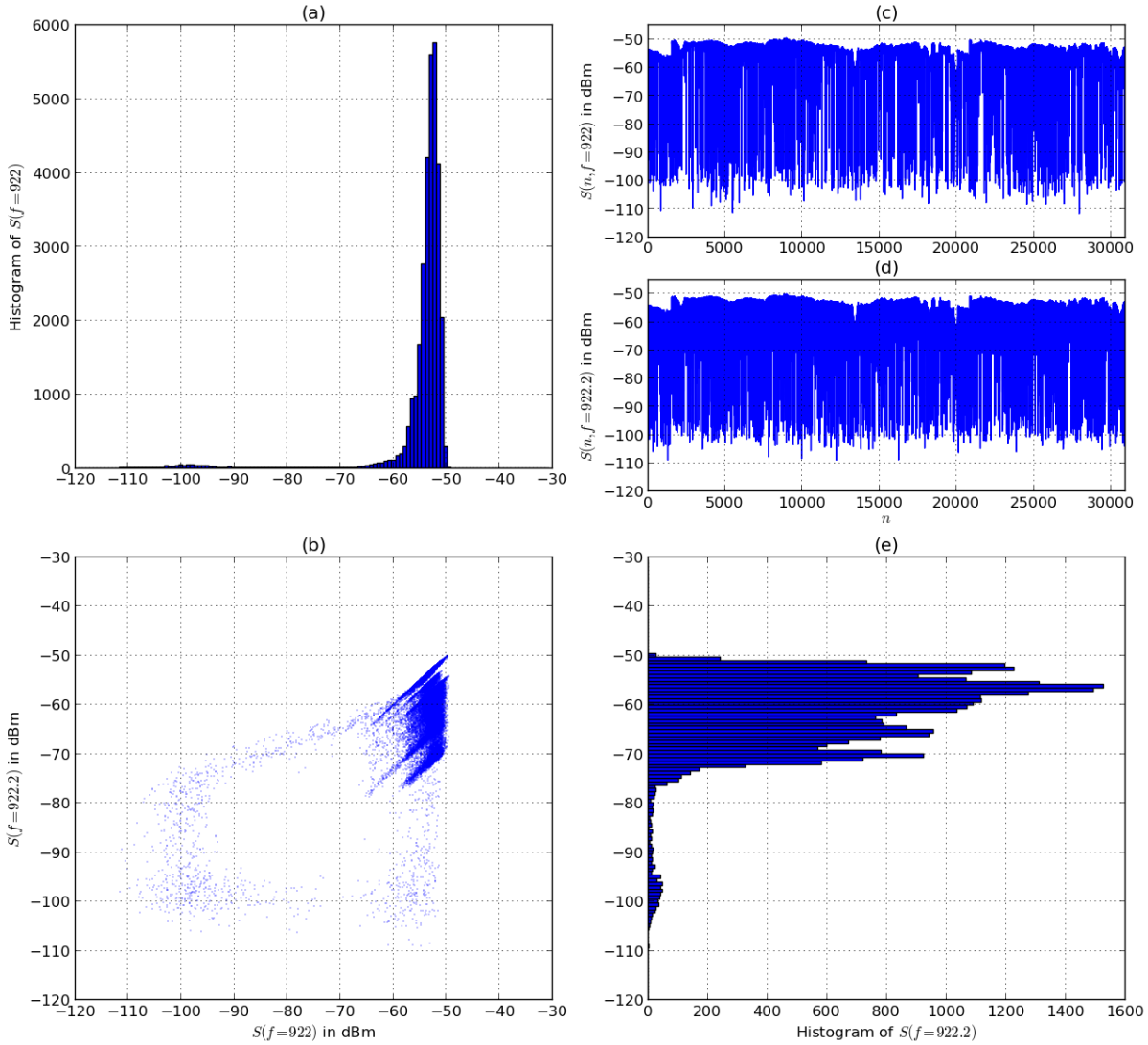


Figure 21 Analysis of two adjacent spectral components in the GSM-R downlink bandwidth for the measurements performed along the LGV East line. (a) and (e) are respectively the histograms of 30929 values of S(f) at f = 922 MHz and at f = 922.2 MHz. (c) and (d) are respectively the 30929 consecutives values of S(f) at f = 922 MHz and at f = 922.2 MHz. (b) is the representation of the joint distribution of S(f) at f = 922 MHz as a function of S(f) at f = 922.2 MHz.

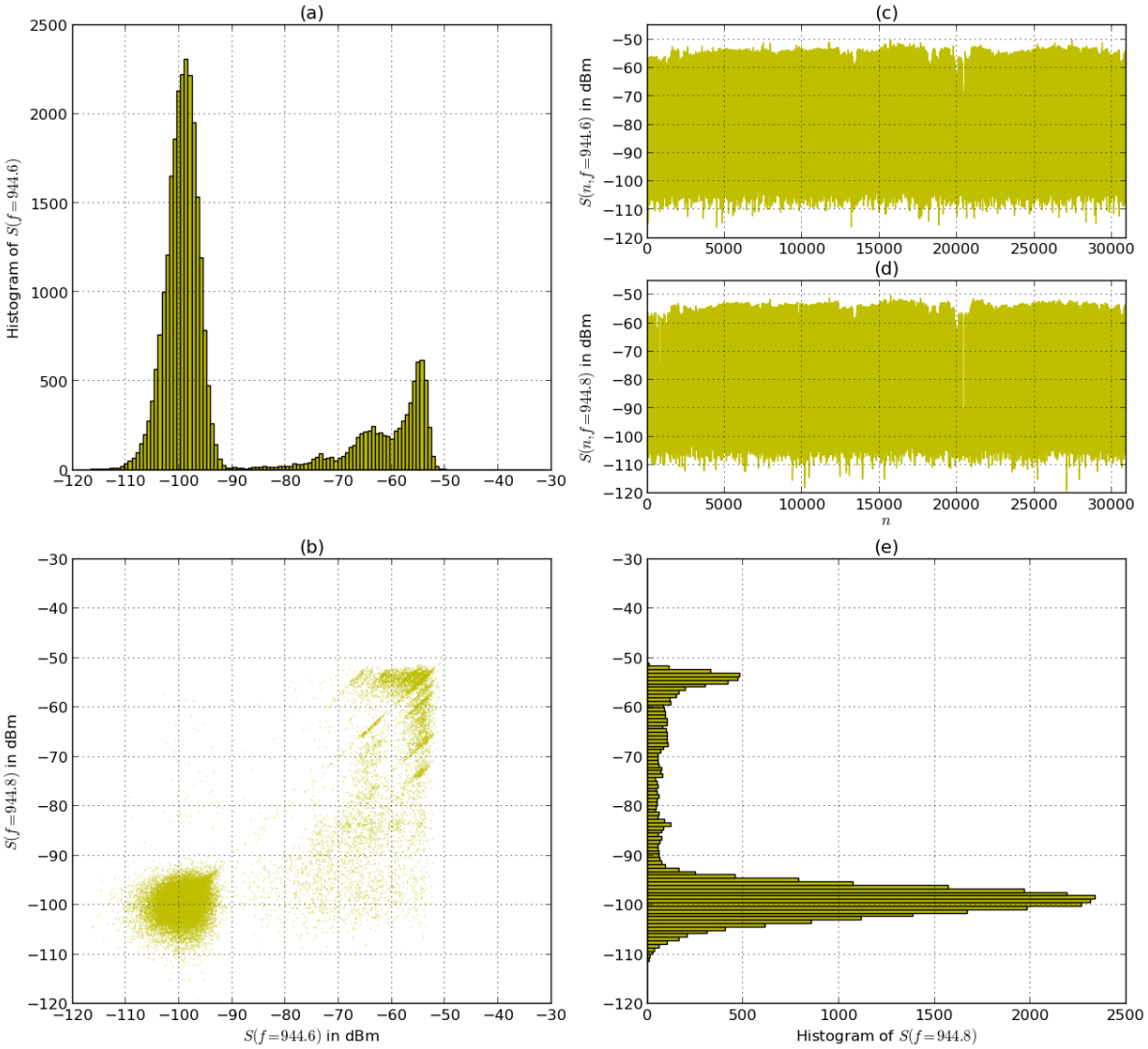


Figure 22 Analysis of two adjacent spectral components in the GSM downlink bandwidth for the measurements performed along the LGV East. (a) and (e) are respectively the histogram of 30929 values of S(f) at f = 944.6 MHz and at f = 944.8 MHz. (c) and (d) are respectively the 30929 consecutives values of S(f) at f = 876 MHz and at f = 944.6 MHz. (b) is the representation of the joint distribution of S(f) at f = 944.6 MHz in function of S(f) at f = 944.8 MHz.

The artefacts of p.s.d. at frequencies f = 922 MHz and f= 922 MHz are singular points being able to degrade the model estimation. In order to eliminate these measurement artefacts, we applied a median filter (order = 11) on the p.s.d. The results are presented respectively for each channel previously analysed in Figure 23, Figure 24 and Figure 25.

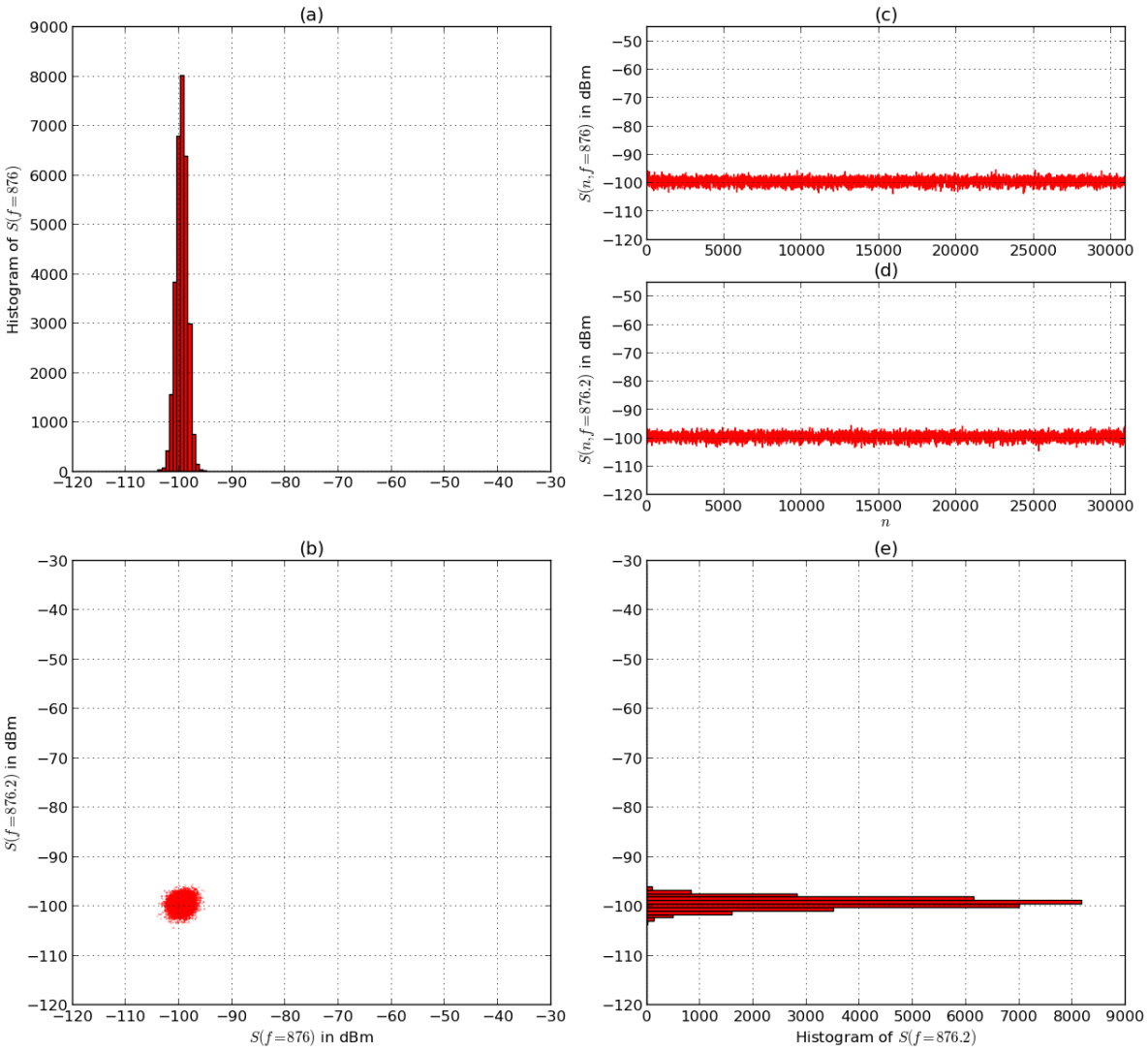


Figure 23 : Analysis of two filtered adjacent spectral components in the GSM-R uplink bandwidth for the measurements performed along the LGV East. (a) and (e) are respectively the histogram of 30929 values of S(f) at f = 876 MHz and at f = 876.2 MHz. (c) and (d) are respectively the 30929 consecutives values of S(f) at f = 876 MHz and at f = 876.2 MHz. (b) is the representation of the joint distribution of S(f) at f = 876 MHz in function of S(f) at f = 876.2 MHz.

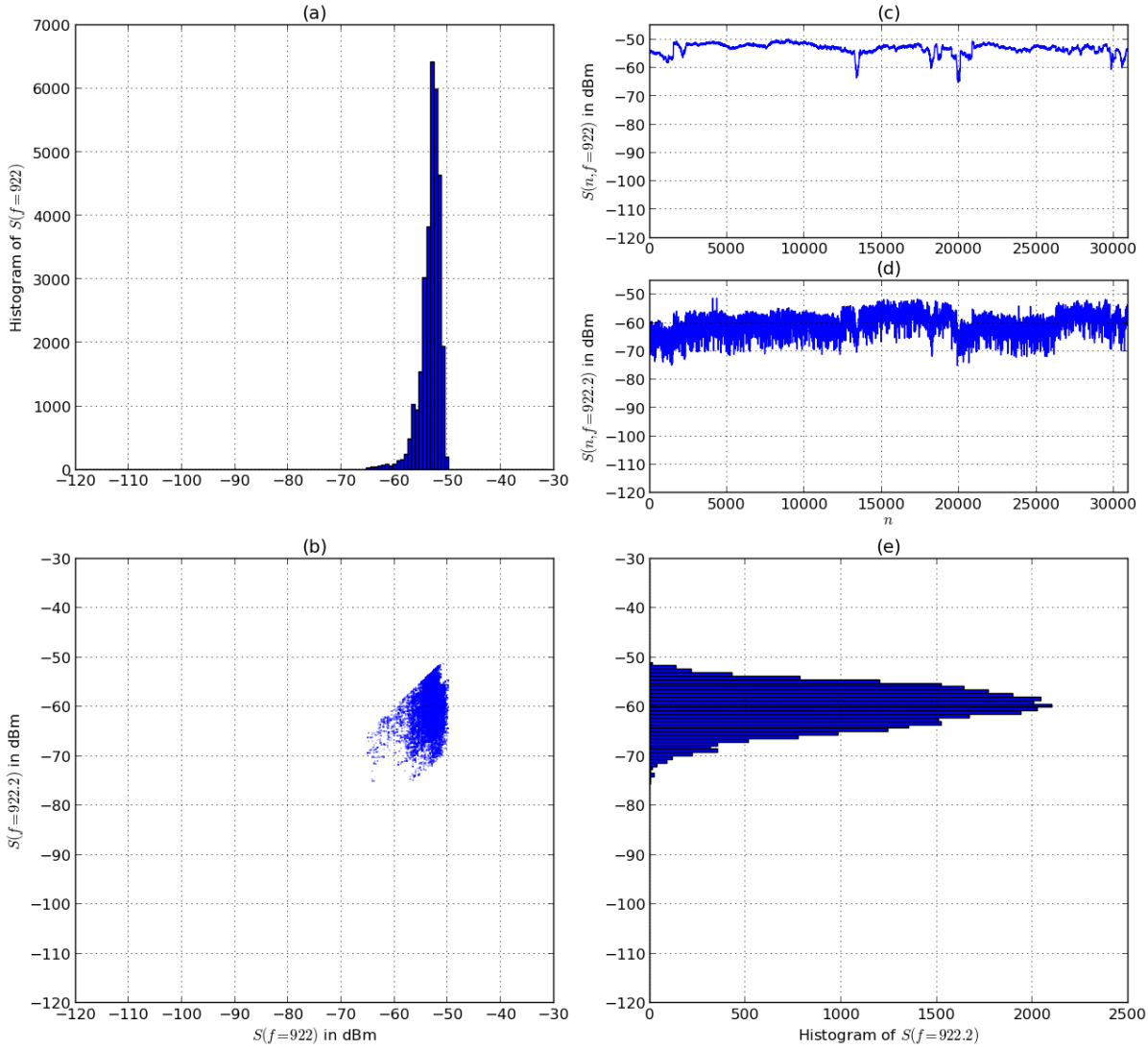


Figure 24 Analysis of two filtered adjacent spectral components in the GSM-R downlink bandwidth for the measurements performed along the LGV Est. (a) and (e) are respectively the histogram of 30929 values of S(f) at f = 922 MHz and at f = 922.2 MHz. (c) and (d) are respectively the 30929 consecutives values of S(f) at f = 922 MHz and at f = 922.2 MHz. (b) is the representation of the joint distribution of S(f) at f = 922 MHz as a function of S(f) at f = 922.2 MHz.

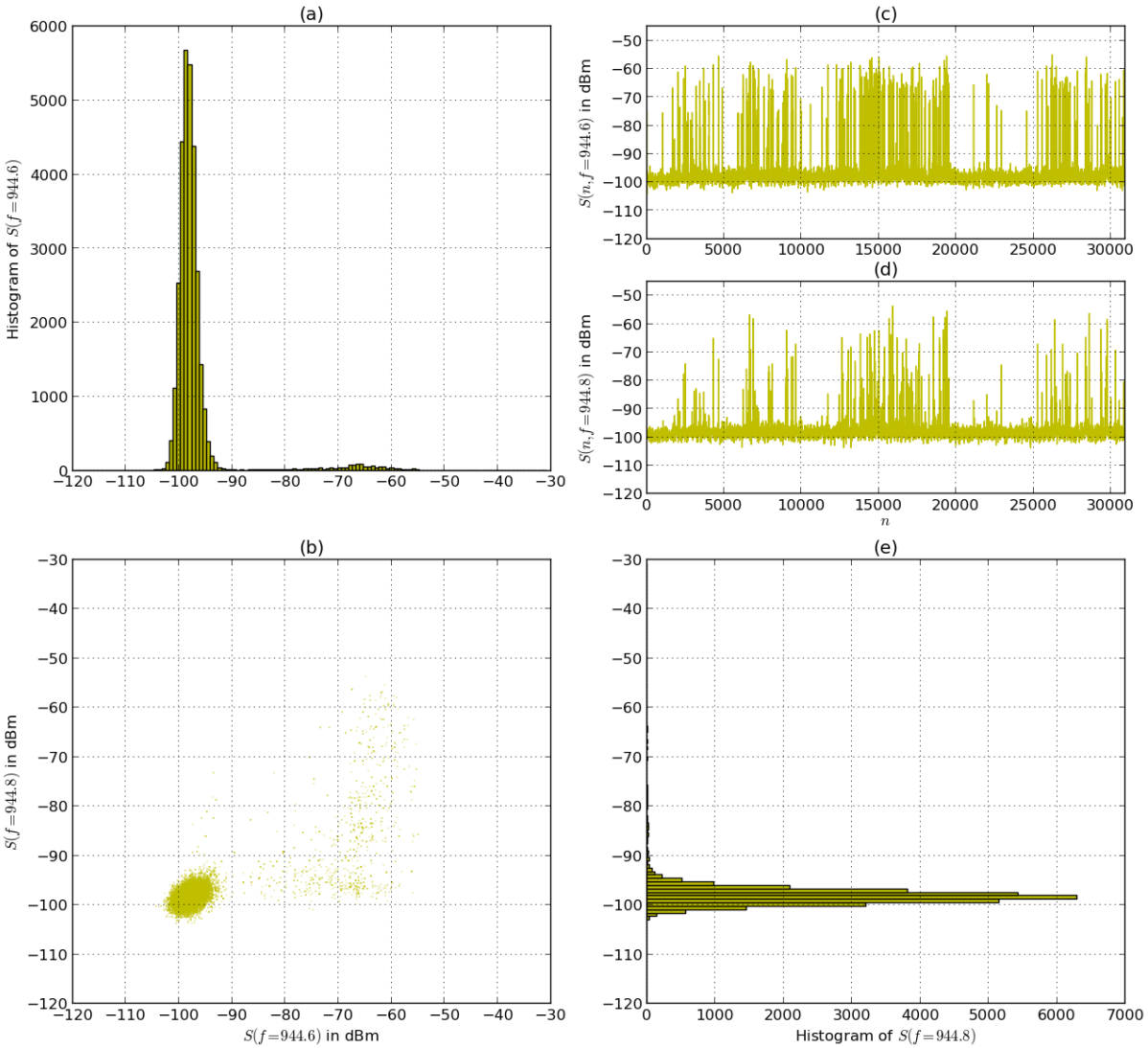


Figure 25 Analysis of two filtered adjacent spectral components in the GSM downlink bandwidth for the measurements performed along the LGV Est. (a) and (e) are respectively the histogram of 30929 values of S(f) at f = 944.6 MHz and at f = 944.8 MHz. (c) and (d) are respectively the 30929 consecutives values of S(f) at f = 876 MHz and at f = 944.6 MHz. (b) is the representation of joint distribution of S(f) at f = 944.6 MHz as a function of S(f) at f = 944.8 MHz.

In the GSM-R uplink bandwidth (Figure 23), the median filter decreases the weakness of p.s.d. values. The histograms are now centred and symmetric. Moreover, their variances are also decreased. In Figure 24, we can show that these artefacts are completely removed. The corresponding histograms have now one mode with variances correctly decreased. However, the effect of the median filter is not always beneficial. If we consider Figure 25, the median filter has deteriorated the mode relative to the communication. Therefore, the median filter could generate difficulties achieving a correct and representative model and in consequence could reduce the ability to detect EM attacks.

5.3. Definition of the EM statistical Model

After performing these necessary preliminary analyses, we chose to build a model of the p.s.d. using a density of Gaussian mixture model. The first idea is that one mode can be represented by one Gaussian kernel. Moreover, the sum of these different Gaussian kernels could be fit, with no symmetric distribution, in increasing the number *G* of kernels. The expression of the Gaussian mixture model (GMM) for the p.s.d **S** of *K* components **S** = [$S(f_0)$… $S(f_{K-1})$] is the following:

$$p(\mathbf{S}) = \sum_{g=1}^{G} p_g N_g(\mathbf{S}; \boldsymbol{\mu}_g, \mathbf{C}_g)$$

with: $0 \le p_g \le 1 \; and \sum_{g=1}^{G} p_g = 1$ (13)

and,

$$N(\mathbf{x}; \boldsymbol{\mu}, \mathbf{C}) = \frac{1}{\sqrt[K]{2pi \det(\mathbf{C})}} \exp\left(-\frac{1}{2} (\mathbf{x} - \boldsymbol{\mu})^t \mathbf{C}^{-1} (\mathbf{x} - \boldsymbol{\mu}) \right) \quad (14)$$

where $N_g()$ is the g^{th} Gaussian kernel defined by its mean vector **μ** and its covariance matrix **C** (cf. the above equation**)**, *G* is the number of Gaussian kernels and p_g weight of each Gaussian kernel in the mixture. We have fixed *K* to 10 components. With a frequency step of 0.2 MHz, a statistical model is defined for a bandwidth of 2 MHz. Finally, we estimate 50 models from f = 875 MHz to f = 975 MHz.

The last model will consider the complex distributions in a precise location but not the variations due to different observation locations. We recall in this context that the spectra are different, due to the presence of different communication signals and/or at different power levels (BTS locations...) and/or the EM environment (difference of train density, difference of the propagation channels (multi-path) of the communication. Regarding this level of complexity, in a first time, our strategy is to build statistical models for each location of observation.

5.4. Detection procedure of the EM attack

The detection implemented in this study is a so-called 'supervised' detection: The detection consists in determining whether each new observed spectrum belongs or not to a stochastic process defined by a generative model estimated on the base of said learning data. In our case, these data represent a said "normal" EM configuration. Assuming that the model is representative of the normal environment, all spectra outside this / these processes will be considered suspect.

In the following, we assume that we have a model of normal environment EM defined as in the previous section. Moreover, we recall that the 'normal' environment model is restricted to the location where the learning data have been acquired.

5.4.1. Frequency local detection

In this subsection, we perform the detection on a frequency bandwidth defined by the frequency bandwidth *K**0.2 used by the models. Since *K*=10, we have M =50 models every 2 MHz. This means that in the overall bandwidth, we evaluate every 2 MHz the EM detection. This is consistent with the wide jamming bandwidth of the jammers identified in WP1.

We consider the m^{th} model $p_m(\mathbf{S}_m)$ corresponding to the band from fmin = 875 MHz + (m-1)*2MHz to fmax = 875 MHz + m*2 MHz. $\mathbf{S}_m$ is a vector of *K* p.s.d. components from fmin to fmax. The detection will consist in evaluating $p_m(\mathbf{S}_m)$ with a new observed spectral vector $\mathbf{S}_m$ and make the following test:

If $p_m(\mathbf{S}_m) > \lambda_m$, $\mathbf{S}_m$ belongs to the model : No EM attack detected
else $\mathbf{S}_m$ does not belong to the model and an EM attack is detected in this frequency band.

More generally, we work with the logarithm of the density of probability:

If $\log p_m(\mathbf{S}_m) > \log \lambda_m$, $\mathbf{S}_m$ belongs to the model : No EM attack detected
else $\mathbf{S}_m$ does not belong to the model and an EM attack is detected in this frequency band.

λ_m is the acceptance threshold determined during the learning phase. It is fixed with a relation using the minimum value of $p_m(\mathbf{S}_m)$ found behind learning data.

5.4.2. Global detection

In this subsection, we make the assumption that the M=50 frequency band vectors are independent between each of them. Under this assumption, the global model of the p.s.d. is equal to:

$$p(\mathbf{S}) = \prod_{m=1}^{M} p_m(\mathbf{S}_m) \tag{15}$$

From this equation, an unique detection for **S** as a whole can be carried out in performing the following test:

$$p(\mathbf{S}) >= \lambda_M \tag{16}$$

As before, λ_M is the threshold. It is determined during the learning phase. The threshold corresponds to the minimum value of $\prod p_m(\mathbf{S}_m)$ obtained with learning data.

Preferring the log version, we obtain:

$$\log\, p(\mathbf{S}) = \sum_{m=1}^{M} \log\, p_m(\mathbf{S}_m) > \log \lambda_M \tag{17}$$

Like previously, if the test is verified then no attack is detected, else the p.s.d. is suspect.

5.4.3. Integration time detection

If the models represent correctly the 'normal' environment, we can use more consecutive spectra to take a decision either in the local test or in the global test. For this, we set the assumption that every spectral channels are consecutively independent in the observation time (the sampling time of acquisition is equal to 3.13 ms). Thus, we can take a decision over *T* consecutive spectra and define the new test in the local detection case as:

$$\sum_{t=0}^{T-1} \log\, p_m(\mathbf{S}_m(t)) > \lambda_{Tm} \tag{18}$$

and in the global detection as:

$$\sum_{t=0}^{T-1} \sum_{m=1}^{M} \log\, p_m(\mathbf{S}_m(t)) > \lambda_{TM} \tag{19}$$

The estimation of λ_{Tm} and λ_{TM} follows the same procedure than in the instantaneous cases. The results of these tests are evidently the same that previously.

5.5. Tests and results

5.5.1. Methodology

5.5.1.1. Learning and test data set

The detection is realized in two phases: The first is the learning phase in order to estimate the probabilistic model of the 'normal' EM environment. The second is the testing phase corresponding to the assessment of the model with jammed and non-jammed spectra sets.

We then cut the p.s.d data measurements in two sets: one set for the learning phase (80 % of the data) and a second one for the test phase (20 % of the data).

For both data sets, as described below, was applied a Median filter with a k = 11 order. The learning phase has been realized with the Expectation Maximization algorithm allowing estimating the different parameter of a GMM: p_g, $\boldsymbol{\mu}_g$ and $\mathbf{C}_g$ [3].

The results of this algorithm depend on the initialization procedure. In consequence, we initialized this algorithm with the SEM algorithm [4]. Finally, we use the Validation Cross principle that consists in cutting the learning data into N subsets and repeating N times the learning phase using N-1 different subsets. Of course, at each learning phase the N-1 subsets are not the same. The selected estimated model is the model performing the maximum likelihood with the N^{th} subset no used. In our case N = 10.

The threshold has been determined by the lowest likelihood value performed by model $p(\mathbf{S})$ in using the learning data set. In following test, we tuned this reference threshold to analyse the method performances:

$$\lambda_{Mc} = \lambda_M + c\lambda_M \tag{20}$$

where c is a scalar. We use the same procedure in the case of integration detection (using λ_{TM}).

5.5.1.2. Perturbation definition

The perturbation has been realized with additive white Gaussian noise. Logically, in order to realize this synthetic disturbed spectrum, we performed this addition in the linear space:

$$X(f) = 20\log_{10}\left(10^{S(f)/20} + b(f)\right) \tag{21}$$

Five patterns of perturbation have been realized according to the frequency bandwidth:

- First Large Band perturbation: 875- 975 MHz (all the p.s.d band)
- Second Large Band perturbation: 875- 921 MHz (GSM-R and GSM uplink and GSM-R downlink are jammed)
- Third Large Band perturbation: 915- 975 MHz (GSM-R and GSM downlink are jammed) Narrow Band perturbation: 915-921 MHz (only the GSM-R downlink is jammed)

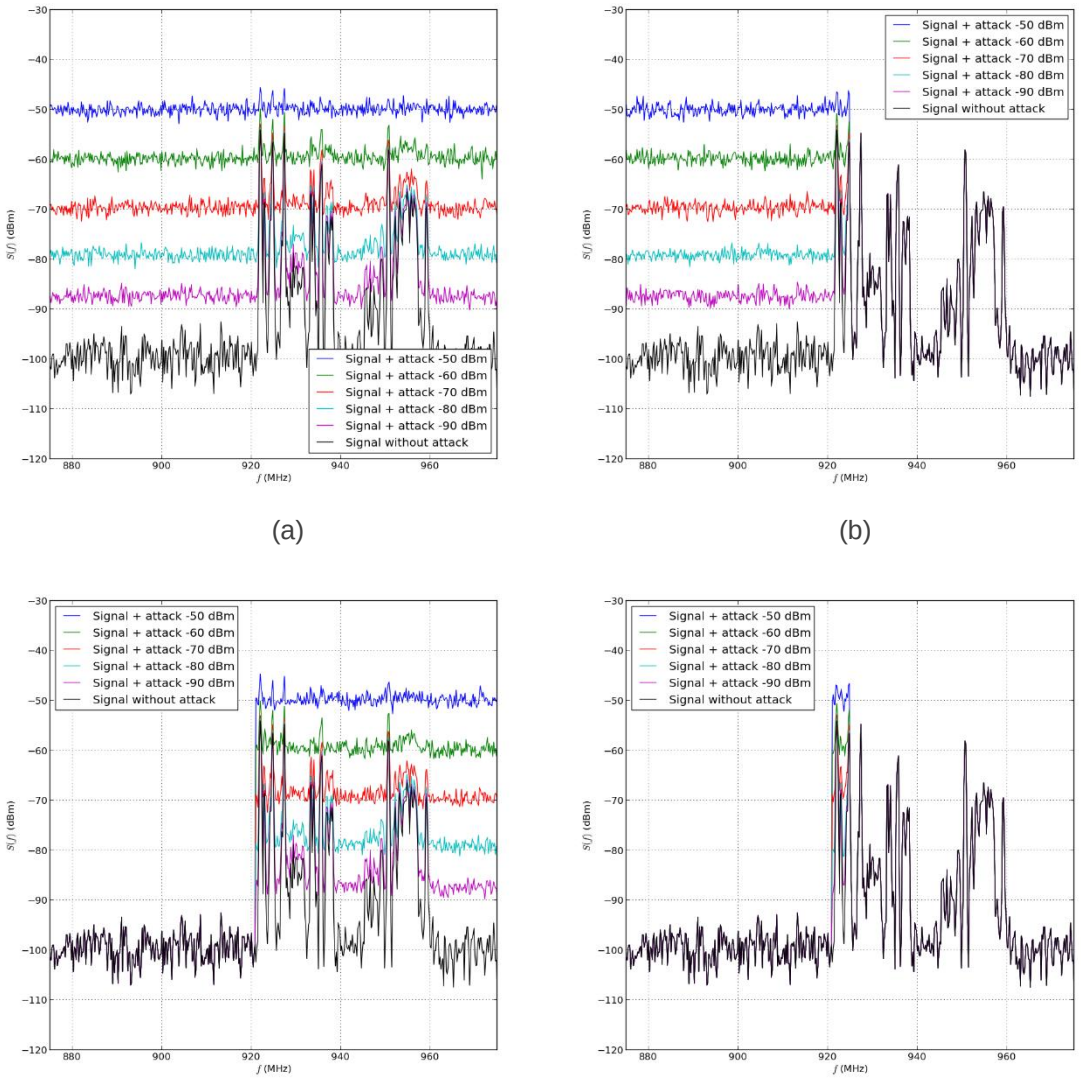


Figure 26. Examples of jammed signals. (a): with the first large band perturbation, (b) with the second and (c) with the third large band perturbation. (d) The jamming signal is the narrow band perturbation.

5.5.2. Detection results

The detection results are presented considering our four railway studied environments. For each environment, the test detection has been performed for the four perturbations previously described above and for 5 levels of power: -50 dBm, -60 dBm, -70 dBm, -80 dBm and -90 dBm.

The results is presented in terms of Good Detection (GD) rates (defined as the ratio between the number of jammed spectra detected and the actual number of jammed spectra) and of False Alarms (FA) rates (defined as the ratio between the number of no jammed spectra detected as jammed and the actual number of jammed spectra).

We used equation 19 to perform the detection. The range of c (equation 20) was set in order to perform a FA = 0% and a GD = 100% for every test cases. Evidently, at each time, the range of c is the same for all power levels of perturbation.

For a better readability of the results, the following tables present the results obtained with the threshold performing, either for GD = 100 % and presenting the FA associated, or for a FA = 0% and presenting the associated GD.

Finally, these results are presented for two times of “integration” T = 1 and T = 10, and for G = 1, 3 and sometimes G=5 number of Gaussian kernels.

5.5.2.1. Large Band perturbations

For each environment and for the three wide band perturbations, the results are similar. Thus, we present in Table 5 and in Table 6 the results only one time. For every cases, an optimum threshold can be tuned to reach perfect results for *T* = 1 and *G* = 1 and this for every power level of synthetic attack signal.

Table 5. Good Detections rate when a threshold is set to obtain a False Alarms rate = 0%.

T=1, *G*=1	FA = 0%				
	-50 dBm	-60 dBm	-70 dBm	-80 dBm	-90 dBm
GD (%) *G*=1	100	100	100	100	100

Table 6. False Alarms rate when a threshold is set to obtain a Good Detection rate = 100%.

T=1, *G*=1	BD = 100%				
	-50 dBm	-60 dBm	-70 dBm	-80 dBm	-90 dBm
FA (%) *G*=1	0.00	0.00	0.00	0.00	0.00

These perturbations are wide band and always cover all the frequency bandwidth without transmission. Thus, in these bands with one mode, the discrimination with a perturbation, even low, is strong. Moreover, the median filter allows achieving the p.s.d. distribution almost equivalent to Gaussian. In consequence, it is not necessary to increase the models complexity for an optimum threshold in these perturbation configurations.

5.5.2.2. Narrow Band perturbations

In the case of narrow band perturbation, the performances are not exactly the same in all EM environments. Although often close, differences exist for the lowest power level. In every case, the stronger score is in bold police. At equal performances, the scores associated to the lowest model complexity is chosen.

5.5.2.2.1. LGV line tests

Table 7. Good Detections rate when a threshold is set to obtain a False Alarms rate = 0%.

		FA = 0%									
		-50 dBm		-60 dBm		-70 dBm		-80 dbm		-90dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
GD (%)	*G*=1	**100**	100	**100**	100	**100**	100	1.01	1.51	0.18	0.25
	G=3	100	100	100	100	100	100	2.92	1.37	0.21	0.16
	G=5	100	100	100	100	100	100	**3.70**	1.43	**0.41**	0.17

Table 8. False Alarms rate when a threshold is set to obtain a Good Detection rate = 100%.

		GD = 100%									
		-50 dBm		-60 dBm		-70 dBm		-80 dbm		-90dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
FA(%)	*G*=1	**0.00**	0.00	**0.00**	0.00	0.07	**0.00**	2.14	1.35	5.37	5.13
	G=3	0.00	0.00	0.00	0.00	**0.00**	0.00	0.22	0.17	0.81	**0.42**
	G=5	0.00	0.00	0.00	0.00	0.00	0.00	0.20	**0.17**	0.64	0.42

For attack power levels of -50 dBm and -60 dBm, the results are perfect for *T*=1 and *G*=1 Gaussian kernel. An exception occurs at -70 dBm, this could imply, either to increase the integration time, or to increase the number of Gaussian kernels to 3. At -80 dBm and -90 dBm (very low power) the FA = 0.0% involves a very low GD rate not exceeding 1.51 % for *G*=1 with *T*=1 or *T*=10. Moreover, the results of GD for *G* = 3 and *G* = 5 are also very low (3.70 at maximum for *G* = 5) and, the integration is not good for both *G* values.

The results presented in Table 8 are most interesting. A performance of GD = 100 % with a FA score maximum of 0.42% (*G*=5, *T*=10). Here the *G*=3 and 5 are little more relevant since, at these levels, the simple case *G*=1 presents a lowest FA rate of 1.35 % (*T*=10).

Both contexts (-80 dBm and -90 dBm) are particular close to the EM noise floor. Moreover, in the GSM-R downlink bandwidth, the number of channels not supporting communication is lower than in the case presented in the previous section. This explains this level of error. Finally, a very good score of GD = 100% is obtained if we accept a tolerance of FA< 1%. A FA = 0% involves a threshold very low, excluding all p.s.d very close to -100 dBm.

5.5.2.2.2. IRIS train tests

The IRIS environment is by definition outside of the hypothesis since the EM environment evolves during the p.s.d acquisition time. We consider that the jamming conditions are stationary. This case is equivalent to a perturbation emitted inside the train with a constant radio link between the jammer situated in the train and the train mounted receiving antenna i.e. fixed jammer in the train in a passenger suitcase for example.

Table 9. Good Detection rate when a threshold is set to obtain a False Alarms rate = 0%.

		FA = 0%									
		-50 dBm		-60 dBm		-70 dBm		-80 dBm		-90 dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
GD (%)	*G*=1	3.70	7.44	1.27	3.31	0.26	0.93	0.12	0.31	0.05	0.00
	G=3	**19.9**	19.6	14.3	16.23	4.48	4.34	1.43	1.03	0.66	0.41
	G=5	19.8	19.8	14.9	**17.9**	3.54	**5.00**	1.40	**1.86**	0.73	**1.24**

Table 10 False Alarms rate when a threshold is set to obtain a Good Detection rate = 100%.

		GD = 100%									
		-50 dBm		-60 dBm		-70 dBm		-80 dBm		-90 dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
FA(%)	*G*=1	42.05	100	75.5	100	99.2	100	100	100	100	100
	G=3	16.3	100	24.22	100	50.9	100	88.7	100	99.6	100
	G=5	**8.00**	100	**19.8**	100	**23.1**	100	**41.7**	100	**89.2**	100

In consequence, the results are not satisfaying. For FA = 0.0 %, the best score is obtained with GD = 19.9 % for an attack of -50 dBm and GD = 17.9 % for -60 dBm power level.

Considering a GD = 100%, we obtain FA = 8% at -50 dBm and FA = 19.8% at -60 dBm. Here, the GMM is better than the mono Gaussian distribution. But the integration is not good due to the environment not being stable (BTS to train antenna link).

5.5.2.2.3. Paris Gare de l'Est station

Table 11 Good Detections rate when a threshold is set to obtain a False Alarms rate = 0%.

		FA = 0%									
		-50 dBm		-60 dBm		-70 dBm		-80 dBm		-90 dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
GD (%)	*G*=1	**100**	100	**100**	100	**100**	100	**100**	100	27.7	89.9
	G=3	100	100	100	100	100	100	100	100	**50**	**93.2**
	G=5	-	-	-	-	-	-	-	-	-	-

Table 12 False Alarms rate when a threshold is set to obtain a Good Detection rate = 100%.

		GD = 100%									
		-50 dBm		-60 dBm		-70 dBm		-80 dBm		-90 dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
FA(%)	*G*=1	**0.00**	0.00	**0.00**	0.00	**0.00**	0.00	**0.00**	0.00	**14.0**	**1.44**
	G=3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	15.1	2.50
	G=5	-	-	-	-	-	-	-	-	-	-

The results are again the same with perfect scores for jamming power signals ranging from -50 dBm to -80 dBm. As concerns the results using *G* = 5 has not been tested in this context. The *G* = 1 and *T*= 10 already providing satisfying results with GD = 100 % if we accept a FA rate of 1.44%. The context *G*=3 is better if we prefer a FA = 0%, but in this case GD = 93.2 %.

5.5.2.2.4. Liège Guillemins station

Table 13 Good Detections rate when a threshold is set to obtain a False Alarms rate = 0%.

		FA = 0%									
		-50 dBm		-60 dBm		-70 dBm		-80 dBm		-90 dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
GD (%)	*G*=1	**100**	100	**100**	100	**100**	100	88.3	100	0.23	0.38
	G=3	100	100	100	100	100	100	**100**	100	2.23	**11.4**
	G=5	100	100	100	100	100	100	93.9	100	0.30	1.89

Table 14 False Alarms rate when a threshold is set to obtain a Good Detection rate = 100%.

		GD = 100%									
		-50 dBm		-60 dBm		-70 dBm		-80 dBm		-90 dBm	
		T		*T*		*T*		*T*		*T*	
		1	10	1	10	1	10	1	10	1	10
FA (%)	*G*=1	**0.00**	0.00	**0.00**	0.00	**0.00**	0.00	0.23	**0.00**	19.9	**10.9**
	G=3	0.00	0.00	0.00	0.00	0.00	0.00	0.04	0.00	20.71	12.2
	G=5	0.00	0.00	0.00	0.00	0.00	0.00	0.23	0.00	26.4	17.4

The results obtained at –50 dBm, -60 dBm and -70 dBm are perfect for *G*=1 and *T*=1. A small difference appear at -80 dBm, corrected either with *G*=3 or *T*=10 for the GD rate (with FA=0.0%) and *T*=10 for the FA rate = 0.0% (with GD = 100%). At -90 dBm, the best GD = 11.4 % with FA = 0.0% is obtained at *G*=3; to obtain a GD = 100 %, FA will reach 10.9% at minimum with *G*=1 and *T*=10.

5.5.3. Results conclusion

Considering these results, we conclude that a model configuration with an integration time *T*= 1 and a number of Gaussian kernels *G* =1 is enough to perform perfect results when jamming power levels are higher than -80 dBm and -90 dBm. Let us remember here that the EIRENE specifications indicate that a minimum useful GSM-R signal is -95 dBm. These results table showed the essential results of ROC curves (FA rate for a GD =100 % and GD rate for FA = 0 %).

The effect of median filter and the high number of channels without signal transmission are the main reason of this performance level. In this context, a refined estimation of models with GMM cannot provide better results. In the case where the optimum threshold is not estimated, and the thresholds are set to the lowest likelihood (equation 20 with *c*=0) obtained with the learning data, the GMM model can perform better results. The following Table 15 presents this test in the LGV East Line environment for the narrow band perturbation.

Table 16. Good Detections rate (%) and False Alarms rate (%) in the LGV Est line EM environment with or not the Narrow band perturbation at several power levels.

	G=1				*G*=3				*G*=5			
	T=1		*T*=10		*T*=1		*T*=10		*T*=1		*T*=10	
	GD	FA	GD	FA	GD	FA	GD	FA	GD	FA	GD	FA
-50 dBm	**100**	**0.00**	100	0.00	100	0.39	100	1.01	100	0.39	100	1.52
-60 dBm	**100**	**0.00**	100	0.00	100	0.39	100	1.01	100	0.39	100	1.52
-70dBm	3.81	**0.00**	5.47	0.00	**100**	0.39	100	1.01	100	0.39	100	1.52
-80 dBm	0.10	**0.00**	0.25	0.00	**100**	0.39	100	1.01	100	0.39	100	1.52
-90 dBM	0.08	**0.00**	0.00	0.00	97.0	0.39	100	1.01	**99.0**	0.39	100	1.52

6. Conclusion

This deliverable D3.3 has presented the research activities performed in WP3, tasks 3.3 and 3.4 of the SECRET project. These tasks aims at identifying each electromagnetic (EM) attack to then insure the efficient resilience of the railway system by providing a reconfigurable radio architecture that is studied in WP4. To detect an electromagnetic attack, we have developed specific recognition systems tuned for different types of EM attacks. The detection principle uses supervised pattern recognition techniques.

Based on this strategy, two different approaches are distinguished and studied in this deliverable.

The first approach consists in performing detection using the train or ground receiving equipment itself. This equipment could be the receiver of a GSM-R transceiver, a TETRA receiving equipment....). To identify the presence of a jammer, we collect the I/Q information directly inside the existing equipment and we select and study two different descriptors. The first descriptor is represented by the radius of the points which composed the I/Q constellation. The second descriptor makes use of the Error Vector Magnitude (EVM) also used to evaluate quality parameters of a radiocommunication. Both descriptors provide effective results in detecting jamming signals superimposed on the communication. The EVM method, already used in telecommunications, could be implemented in a receiver with a special processing to deliver an alarm which can then be used by the Health Attack Manager developed in WP4.

The second approach is conducted in parallel with the existing receiving chain. It is based on the supervision of the radiofrequency spectrum in the band of interest. It uses separate equipment connected to the antenna receiver. This equipment can also be a specific processing in the case a full digital receiver is used. Full digital receivers, i.e. software defined radios, are not yet commonly used by the railway industry. We perform the detection of attacks by an adapted frequency analysis based of the previous knowledge of the normal electromagnetic environments corresponding to the system in use. We use power spectral densities composed of M spectral channels sampled over a bandwidth covering the railway operator band of interest. We build different models for p.s.d. covering a limited bandwidth for each of the considered railway environments i.e. railway line, station, train. The results, presented in terms of Good Detection rates and of False Alarms rates also demonstrate the interest and validity of this second approach. This second approach provides also effective results in detecting jamming spectrums superimposed on 'normal' environment spectrums.

7. Acknowledgements

The authors deeply thank the railways operators SNCF and SNCB for providing authorization and support during the measurement phases analyzed in this deliverable.

8. References

[1] EIRENE System Requirements Specification version 15.3.0

[2] R. A. Shafik, S. Rahman, R. Islam and N. S. Ashraf, On the Error Vector Magnitude as a Performance Metric and Comparative Analysis, International Conference on Emerging Technologies (ICET), pp. 27–31, 13-14, November 2006.

[3] A.P. Dempster, N.M. Laird and D. Rubin, Maximum Likelihood from Incomplete Data via the EM Algorithm, Journal of the Royal Statistical Society. Series B (Methodological), vol. 39, no 1, 1977, p. 1–38 (JSTOR 2984875)

[4] G. Celeux et G. Diebolt, The sem algorithm : a probabilistic teacher algorithm derived from the em algorithm for the mixture problem, Rapport de recherche RR-1364, Inria, Institut National de Recherche en Informatique et en Automatique, 1985.