Uncertainty analysis in system-level vulnerability assessment for IEMI

Recognition Process of Jamming Signals Superimposed on GSM-R Radiocommunications

S. Mili, D. Sodoyer, V. Deniau, M. Heddebaut
Univ.Lille Nord de France, IFSTTAR,
Villeneuve d'Ascq, France
souheir.mili@ifsttar.fr

H. Philippe
SNCF
La Plaine Saint-Denis, France
henri.philippe@sncf.fr

F. Canavero,
Dipartimento di Elettronica e Telecomunicazioni, Politecnico di Torino
Torino, Italy

***Abstract*— This paper explores an approach trying to recognize the presence of electromagnetic attacks on an equipment. Wireless communications are widely used in railway traffic management systems. Such systems are probably susceptible to be disturbed by malicious actions involving jammers. The general objective of this work is to develop a specific method enabling to detect and to recognize these types of interfering signals. This method could be used to involve adequate reactions in order to reduce the impact on the railway network. This paper focuses on the recognition method. It is based on accurate statistical models of signals generated by jammers. This work is carried out in the framework of the European project "SECRET" for SECurity of Railways against Electromagnetic aTtacks.**

Keywords—Electromagnetic attack; jammer; radio communication; detection; GSM-R

I. INTRODUCTION

Nowadays, on the shelf jamming devices are becoming easier to obtain and they could be used for malicious attacks aiming to disturb radio communication dedicated to operational purposes.

The impact that could have these jamming devices on radio communication is also studied in the railway domain. Indeed, the European Rail Traffic Management System (ERTMS), answering to the strong need for railway interoperability throughout the European Rail Network, and designing a unique European Train Control System (ETCS), makes use of a large wireless telecommunication network. Such a system needs to be resilient to electromagnetic jamming devices.

The ETCS system considers two important components. The "Eurobalise" system is used for spot communication as well as train localization [1]. The digital radio system "Euroradio" is based on the Global System for Mobile communication – Railways (GSM-R). It allows the exchange of voice as well as railway signalling data between trains and control centers [2].

Our study focuses on the GSM-Railway communication system using the European frequency band 876 MHz to 915 MHz for the uplink and 921 MHz to 960 MHz for the downlink. The final goal is to evaluate the GSM-R resilience against potential attacks from jamming radio signals. One particular class of jammers consists in devices able to disturb radio communication by transmitting EM signals and sharing the same frequency band. They generate RF signals at sufficient power levels to be of the order of magnitude of the useful signals. Knowing that the received power at the train antenna ranges between -20 dBm and -90 dBm [3], it becomes therefore realistic to achieve this situation with sufficiently close, limited power jammers. The detection and recognition of such disturbing signals require adapted approaches [4].

This paper proposes a specific approach based on statistical study. This study considers that the power spectral density (psd) of the signal jammers can be modelled by a probabilistic density function (pdf). In this way, we obtain different kinds of pdf, allowing us a possible robust classification of the different available jammers.

This paper is organised the following way. A brief presentation of the existing jammer classes is recalled. Then, to facilitate the identification of an effective theoretical tool able to solve this recognition problem, a preliminary laboratory experiment is presented and its results are analysed. The following section is dedicated to the presentation and the developments related to the considered theoretical recognition tool. The next section explores the effectiveness of this tool using experimental results obtained from a dedicated test bench. Finally, conclusions and future works are provided concerning the project.

II. JAMMERS CLASSES

A study was carried out regarding the existing jammers. Five classes of scrambling jammers were identified noted A to E [5]:

Type 'A' devices 'jammers': These devices hold several independent oscillators transmitting 'jamming signals' disturbing and making impossible the establishment of the

communications, blocking the frequencies used by mobile communication equipment.

Type 'B' devices 'intelligent cellular disablers': These devices do not transmit interfering signals but work as detectors. So, when they detect signals in quiet areas, they send a signal to inform the base station to interrupt the communication.

Type 'C' devices 'intelligent beacon disablers' : These devices work on the control channels as 'beacons', they control mobile devices located in a quiet area by sending instructions to disable ringer or disable its operation.

Type 'D' devices 'Direct Receive and Transmit Jammers': These devices operate as a small independent base station. The jammer is predominantly in receiving mode and will choose intelligently interaction and blocking the cell phone if it is within close proximity of the jammer.

Type 'E' devices 'EMI Shield – Passive Jamming': These jamming solutions consist in the suppression of electromagnetic signals by using the properties of the Faraday cages. The Faraday cage essentially blocks, or greatly attenuates, all electromagnetic signals entering or leaving the cage.

In this paper, we consider type 'A' of jammers.

III. Preliminary Experimental Analysis

Jammer signal ratio (JSR) is used to evaluate the impact of a jammer on a system. A conventionally rule of thumb used for FM voice as well as for data systems, not protected by spread spectrum techniques, is that a jammer signal ratio (JSR) of 1 leads to significant degradation of performance and that a JSR greater than 2 leads to an almost total loss of performance [6].

Considering this JSR scale, we study the immunity of the GSM-R by testing the quality of the communication affected by the disturbance attacks. Type 'A' jammers used in our study are continuous wave (CW) transmitters sweeping very fast the whole targeted frequency range.

The impact of such a jammer depends on the relative signal strengths provided by the jammers and from the distant useful communication transmitter present at the input of the receiver [7]. This power depends on the effective radiated power generated by the transmitters and of their relative distance. The effects of the jamming affect the quality of the communication in terms of bit error rate (BER) and, as a consequence, the level of the corresponding JSR [8].

Experiments performed in laboratory have shown that the jamming signal 'A' is typically generated by modulating the transmitter voltage control oscillator (VCO) of a transmitter using a ramp signal to sweep the full targeted frequency band [9]. It also appears that these devices do not implement any stability frequency control system like a phase locked loop (PLL). Therefore, the frequency stability of these devices is limited and, as a consequence, the overall output spectrum is also not very stable along time and temperature [6].

Using these inputs, we consider different interfering signals and we evaluate their effects on the BER, varying their JSR. Using the laboratory test bench presented in Fig. 1, we consider a GSM-R communication established on a specific channel, at a frequency (f_1). We then add different interfering CW signals coming from a signal generator and evaluate their impact using a GSM-R protocol emulator and analyser noted CMU in Fig. 1.

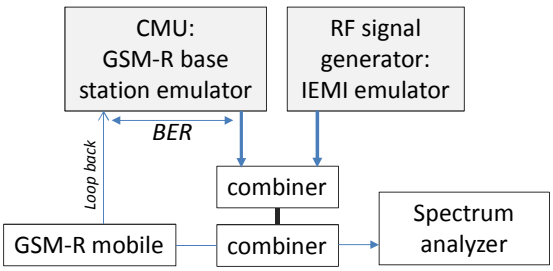

Fig. 1. GSM-R transmitter Test bench.

In this paper, we consider two interfering signals. The first one is a pure CW sinusoidal signal centred in the used GSM-R channel. The second interfering signal is a FM modulated sinusoidal signal whose excursion is set to 75 kHz, also centred on the used 200 kHz wide GSM-R channel. In Fig. 2, we represent the spectral power density of these different signals centred at 924.8MHz.

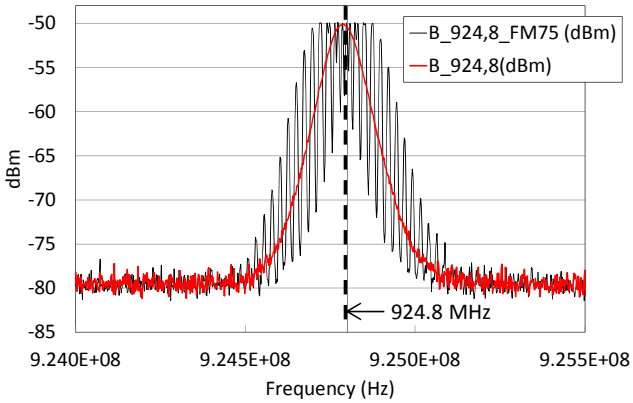

Fig. 2. GMSK transmitted PSD representations of generated signal to disturb the communication

The simulation results are regrouped in table 1. The used power levels delivered by the GSM-R transmitter and the jammer are respectively indicated in columns 1 and 2. The resulting JSR is indicated in column 3 and the corresponding BER for the pure CW jammer and the FM modulated jammer are respectively indicated in columns 4 and 5.

"Loss of communication" (Loss of com. in table I) means that the communication is lost after applying the disturbing signal. No connection (No con.) means that no GSM-R connection at all can be established when the jammer signal is applied.

In these experimental conditions, we obtain that using almost equivalent received powers between the useful GSM-R signal and the jammer signal lead to severe problems for the communication; a pure CW signal is less critical than a FM modulated signal. We specified that without jamming the BER of the communication is equal to 0.

TABLE I.

P_GSM-R (dBm)	P_JAM (dBm)	JSR (dB)	BER_*fl*	BER_FM 75
-38	-36	2	Loss com	No con
-38	-37	1	12,585	No con
-38	-38	0	5,564	No con
-38	-40	-2	2,126	14,662
-38	-42	-4	0,771	7,814
-38	-44	-6	0,256	2,719
-38	-46	-8	0,114	0,588
-38	-48	-10	0,06	0,155
-38	-50	-12	0,023	0,038

Therefore, to conclude on this preliminary phase, an effective recognition model cannot easily be developed using only the received power information. A more sophisticated approach based, for example, on the power spectral density (psd) of the signal jammers could be necessary. This theoretical approach is now presented in the following section.

IV. STATISTICAL MODEL AND RECOGNITION

A. Statistical model definition

We propose to model the spectrum of jammer by a probabilistic model. Considering that spectral components are independent, the pdf of the spectrum associated to a jammer J_k is defined as following:

$$p(\mathbf{S}/J_k) = \prod_{n=1}^{N} p_{\mathrm{f_n}}\left(S(f_n)/J_k\right) \tag{1}$$

where S represent a vector of N spectral components S(fn) of psd expressed in dBm, n∈ [1, N] and $p_{\mathrm{f_n}}(S(f_n)/J_k)$ is the marginal pdf of each component $S(f_n)$. At first, we consider a basic theoretical issue assuming $S(f_n)$ follows a Gaussian statistical law:

$$p_{\mathrm{f_n}}\left(S(f_n)/J_k\right) = \mathcal{N}(S(f_n)/J_k;\mu_{f_n},\sigma_{f_n}) \tag{2}$$

with

$$\mathcal{N}(x;\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right) \tag{3}$$

where μ and σ represent respectively the mean and the standard deviation of the Gaussian random variable x [10]. In order to improve the model, we propose to use a more complex model using a Gaussian mixture distribution:

$$p_{\mathrm{f_n}}\left(S(f_n)/J_k\right) = \sum_{g=1}^{G} p_g \mathcal{N}_g(S(f_n)/J_k;\mu_{g,f_n},\sigma_{g,f_n}) \tag{4}$$

where G is the number of Gaussian kernels and p_g is the weight of the g Gaussian kernel in the mixture (p_g>0 for all g and $\sum_{g=1}^{G} p_g = 1$).

For each kind of EM Attack, a statistical model defined by (2) or (4) is learning and then used in the recognition procedure.

B. EM attack recognition

This work adopts the framework of supervised pattern recognition. In this way, a principle of Bayesian classifier is used: Considering K *(K = 3)* kinds of EM attack, $p(\mathbf{S}/J_k)$ represents the statistic model of the EM attack k (k∈ [1, K], *k=1 for jammer1, k=2 for jammer2 k=3 for jammer3*).

From the Bayes theorem [10]:

$$\begin{aligned} p(\mathbf{S},J_k) &= p(J_k)p(\mathbf{S}/J_k) \\ &= p(\mathbf{S})p(J_k/\mathbf{S}) \end{aligned} \tag{5}$$

and knowing that $p(\mathbf{S}) = \int_J p(\mathbf{S},J)dJ$, the *a posteriori* probability that the realization **S** belongs to the class J_k from the total existing K class is:

$$p(J_k/\mathbf{S}) = \frac{p(J_k)p(\mathbf{S}/J_k)}{\sum_{l=1}^{K} p(J_l)p(\mathbf{S}/J_l)} \tag{6}$$

Considering that each EM attack k is equiprobable, (i.e. $p(J_k) = 1/K$, for all k), the "recognized" EM attack for a spectral observation S maximizes the following relation:

$$\hat{J}_k = \arg\max_{i\in[1,K]} \frac{p(\mathbf{S}/J_i)}{\sum_{l=1}^{K} p(\mathbf{S}/J_l)} \tag{7}$$

In (7) the maximized function varies between 0 and 1; it is equivalent to the Maximum a posteriori (MAP), equal, in this case to the Maximum Likelihood (ML).

V. EXPERIMENTATIONS

A. Data Base

The scheme on Fig. 3 represents the test bench used for the acquisition of the databases necessary for the learning and test phases. This test bench is similar to those presented in section III, where all of the connections are wired, except that the signal generator is replaced by a real jamming device as the interference signal.

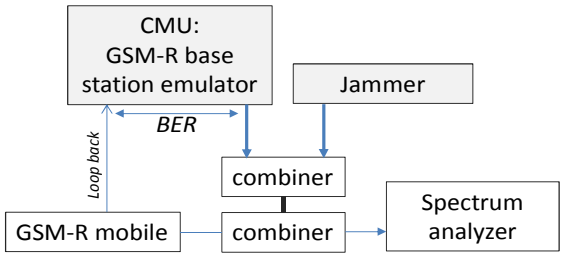

Fig. 3. GSM-R Test bench with GSM jammer.

The data base is constituted of the observations of the frequency spectrum in different contexts. The first context (C1) considers the presence of jamming signals only. The acquisition is realized in two steps, the first step for the learning phase and the second step for the test phase. Three widespread representative jammer devices are used.

The second context (C2) considers the observations of a GSM-R signal and an added jamming signal, using also the three available devices.

Every data is recording during 30 sec with a sample frequency of 100 ms. For each type of signal used for learning or for testing, we get 300 observations. This means that each frequency contained on the PSD has 300 observations. We evaluate the spectrum of the different signals on a frequency band going from 850 MHz to 1 GHz and with a sampling frequency of 0.1 MHz, we obtain 1501 frequency points. Fig. 4 presents an example of spectrum realisation for the three used devices, $K = 3$.

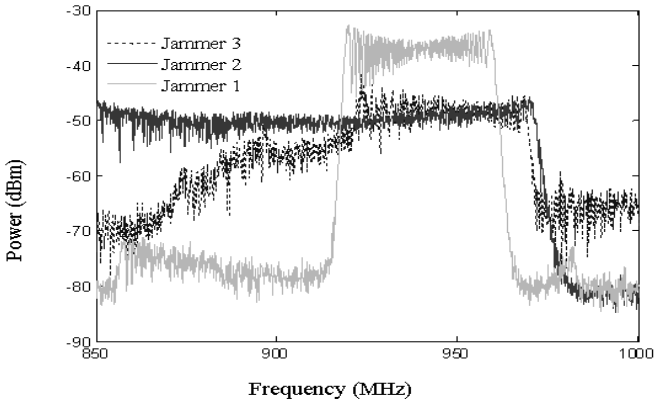

Fig. 4. PSD representation of the Jammers signals.

B. *Learning Phase*

The learning phase consists in estimating the different parameters of the statistic model p(S/Jk) defined by (2) or by (4) for three jammers ($1 \leq k \leq K$) and, using a database C1.

For the Gaussian model (2), we estimate the mean μ_{fn} and the σ_{fn} for each N=1501 frequency (f_1=850 MHz … f_N=1GHz). For the statistic model using the Gaussian mixture model (GMM) (4) we estimate for all the N frequency, the parameters of each G Gaussian kernel: $p_{g,fn}$, $\mu_{g,fn}$ and $\sigma_{g,fn}$. This estimation is realised by the implementation of the Expectation-Maximisation algorithm (EM) [11]. We consider in this work several GMM, i.e. $G = 2$, 3 and 4.

In order to evaluate the matching fit of these different models, we use the X^2 test of goodness of fit [12]. It consists in estimating:

$$X^2 = M \sum_{i=1}^{I} \frac{(h_i(x) - p_i(x))^2}{p_i(x)} \qquad (8)$$

where $h_i(x)$ is the observed distribution (histogram of x) decomposed in I intervals and $p_i(x)$ is the estimated distribution evaluated for x evolved in the interval i. Expression (8) implies that the more X^2 is small, the more the $p_i(x)$ matching fits with the distribution of the variable x. A critical threshold can be used to reject or accept the hypothesis that x follows the tested law, see [12] for more details.

Fig. 5 and Fig. 6 present results of the estimated models for one jamming device (k=1) and respectively for the frequency f_1= 861.9 MHz and the frequency f_2=924.8 MHz. For both frequencies we can observed that the Gaussian model is not adapted to fit correctly the distribution of the data. This is more significant for the frequency f_1= 861.9 MHz: the Gaussian model being symmetric, it cannot model the dissymmetry of data distribution, being generally the case for spectral components in dBm.

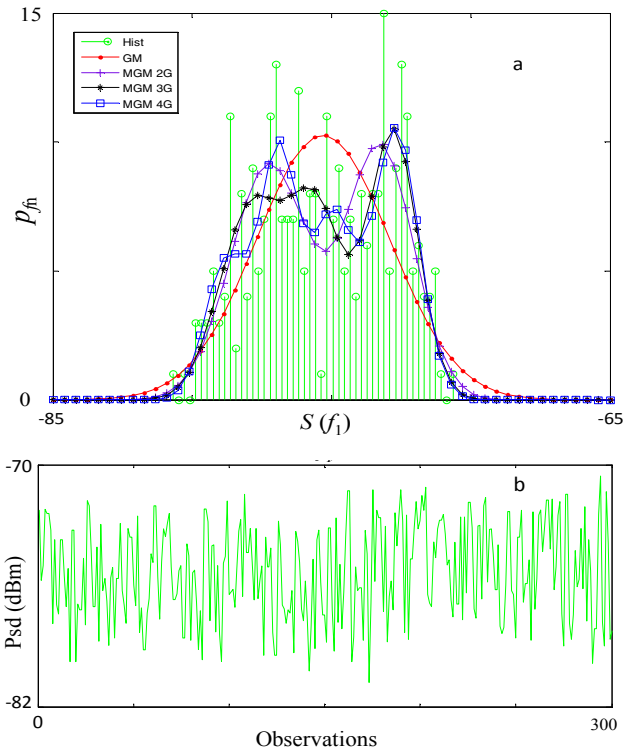

Fig. 5. a. Histogram and Pdf of frequency f_1=861.9 MHz for Gaussian model and MultiGaussian with G=2,3,4. b. PSD Observations of the frequency f_1.

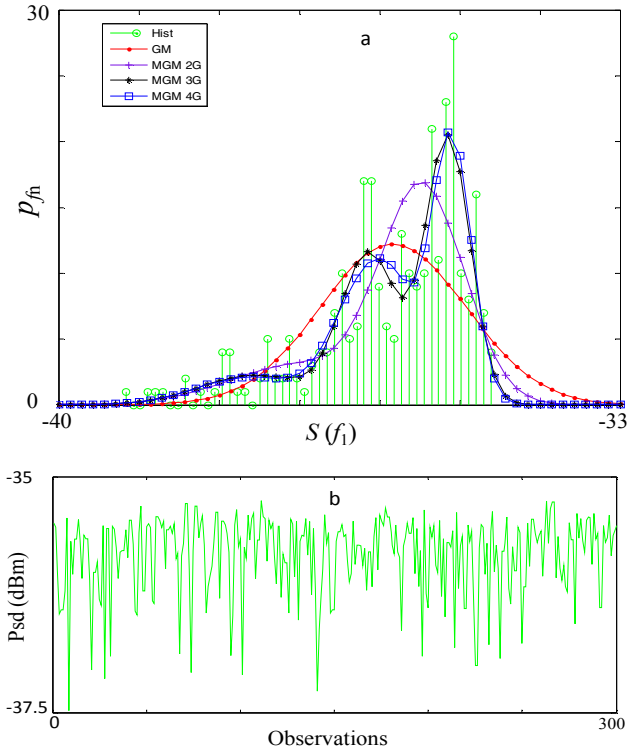

Fig. 6. a .Histogram and Pdf of frequency f_2= 924.8 MHz for gaussian model and MultiGaussian with G=2,3,4. b . PSD Observations of the frequency f_2.

Fig. 7 presents the results of χ^2 test carried out on the N marginal distributions of (1). The results are presented in ascending order. Fig. 7 shows the errors are more significant for the Gaussian model than the GMM model. However, none model has been rejected for a test realized with a 5% confidence level, due to the large number of considered frequencies. In this test, we can see that the best model is described by the GMM model with $G = 4$ Gaussian kernels.

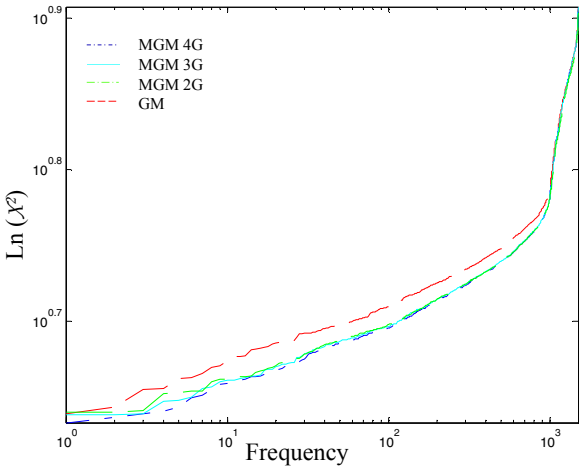

Fig. 7. Logarithmic scale of ln (χ^2) with stored frequencies for Gaussian model and MultiGaussian with G=2,3,4.

C. *Recognition EM attack test*

Considering the equation (7), we tested the capability of our models to recognize the EM attack. All the observation tests (300 for each tested jammer) are preliminary evaluated by (7) to estimate the jammer used. We considered two spectral condition experiments: the first one considers the spectral observations from f_1=850 MHz to f_N=1GHz and the second one considers a shorter frequency band corresponding to the GSM-R downlink frequency band: f_1= 921MHz to f_N = 925MHz. The results obtained with the Gaussian model are presented in Table 2 and the results given by the GMM model with $G = 4$, which is the best one according to χ^2 test, are given in Table 3, for the contest C1. Tables 4 and 5 present the results for both models in the context C2. In the tables, the lines represent respectively the k^{th} jammer used (k = 1,2,3), whereas the columns indicate the identification rate for each jammer. Note that recognition is perfect when the "matrix" is diagonal.

TABLE II. TEST RESULTS (IN %) FOR THE CONTEXT C1 WITH GAUSSIAN MODEL, (A) FOR THE FREQUENCY BAND: F_1=850 MHZ TO F_N =1GHZ, (B) FREQUENCY BAND: F_1= 921MHZ TO F_N = 925MHZ.

	***k*=1**	***k*=2**	***k*=2**
k=1	100	0	0
k=2	0	100	0
k=3	0	0	100

a

	***k*=1**	***k*=2**	***k*=2**
k=1	100	0	0
k=2	0	100	0
k=3	0	0	100

b

TABLE III. TEST RESULTS (IN %) FOR THE CONTEXT C1 WITH GAUSSIAN MIXTURE MODEL, (A) FOR THE FREQUENCY BAND: F_1=850 MHZ TO F_N =1GHZ, (B) FREQUENCY BAND: F_1= 921MHZ TO F_N = 925MHZ.

	***k*=1**	***k*=2**	***k*=2**
k=1	100	0	0
k=2	0	100	0
k=3	0	0	100

a

	***k*=1**	***k*=2**	***k*=2**
k=1	100	0	0
k=2	0	100	0
k=3	0	0	100

b

TABLE IV. TEST RESULTS (IN %) FOR THE CONTEXT C2 WITH GAUSSIAN MODEL, (A) FOR THE FREQUENCY BAND: F_1=850 MHZ TO F_N =1GHZ, (B) FREQUENCY BAND: F_1= 921MHZ TO F_N = 925MHZ.

	***k*=1**	***k*=2**	***k*=2**
k=1	100	0	0
k=2	0	100	0
k=3	0	0	100

a

	***k*=1**	***k*=2**	***k*=2**
k=1	34	66	0
k=2	0	100	0
k=3	0	31.7	68.3

b

TABLE V. TEST RESULTS (IN %) FOR THE CONTEXT C2 WITH GAUSSIAN MIXTURE MODEL, (A) FOR THE FREQUENCY BAND: F_1=850 MHZ TO F_N =1GHZ, (B) FREQUENCY BAND: F_1= 921MHZ TO F_N = 925MHZ.

	***k*=1**	***k*=2**	***k*=2**
k=1	100	0	0
k=2	0	100	0
k=3	0	0	100

a

	***k*=1**	***k*=2**	***k*=2**
k=1	60	40	0
k=2	0	100	0
k=3	0	50.3	49.7

b

Tables 2 and 3 show excellent results obtained by the recognition function (7) when we use a signal only composed by jamming signal at each observation tested ("test" database C1). This success is verified for all statistical models (i.e., (2) and (4) for $G = 4$) and for both widths of frequency band. This is explained by the significant differences between the spectrums of jamming signals. For example, in Fig. 4, although the spectrums of the jammers 2 and 3 are similar in the 920 MHz-970 MHz frequency band, there are significantly different over the other frequencies. When the width of the observation frequency band is reduced (Table 2 (b) and 3(b)), Fig. 4 shows that the spectrums of jamming signals are also sufficiently different to obtain a high discrimination between the different jammers.

The results of the test recognition carried out in presence of communication signal superimposed to the jamming signal ("case the most natural") are presented in tables 4 and 5. Once again, the performances between both models are equivalent. The table 4(a) and 5(a) present excellent results which can be explained by the narrow frequency band of the communication signal in relation to the observation frequency band taking into account in the model of jamming signals. However, the results are less satisfying in the tables 4(b) and 5(b), for which the observation frequency band is significantly covered by the communication signal. In consequences, the recognition of the jamming device is seriously affected.

VI. CONCLUSION

This paper studied an approach trying to recognize the presence of electromagnetic attacks on communication equipment. Starting by the presentation of the different existing classes of jammers, it has then focused on CW wideband jammers. We obtained that, using almost equivalent received powers for a useful GSM-R signal and for the jammer, severe problems are encountered by the communication. Therefore, an effective recognition model could be hardly established based only on the discrimination of the received power levels and, a more sophisticated approach based on the power spectral density of the signal jammers was presented. By its supervised nature, this recognition processing has been decomposed in two steps: one for the learning models able to represent the distribution of different EM attacks, and a second one for the phase of recognition based on the learned model. We have tested different kinds of statistical models, which provided excellent results in terms of recognition if they are estimated on a relatively large frequency band and not only on the down-link GSM-R frequency band.

This work carried out in controlled and simplified conditions (no reflections, no environmental EM noise) was a necessary preliminary study to characterise the jammer signals and their impact on communication systems. It allowed building fundamental bases for the problem of the EM Attacks recognition. Future works will consist in completing this recognition process as well as working on the detection method. Naturally, the perspective of EM attacks recognition study will be to consider more realistic conditions and a larger database of EM attacks kinds. In these conditions, the processing procedure will be more sophisticated and should consider the possible variations of the EM environment in which the GSM-R communication system evolves.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Community's Framework Program FP7/2007-2013 under grant agreement n°"285136".

REFERENCES

[1] D. Mansson, R. Thottappillil, M. Bäckström and O. Lundén, "Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI," IEEE Transactions on Electromagnetic Compatibility, vol. 50, no. 1, pp. 101−109, 2008.

[2] S. Midya and R. Thottappillil, "An Overview of Electromagnetic Compatibility Challenges in European Rail Traffic Management System", Journal of Transportation Research Part C: Emerging Technologies, Elsevier, (Ed.), Vol.16C, pp. 515-534, 2008.

[3] T. Hammi, N. Ben Slimen, V. Deniau, J. Rioult and S. Dudoyer, "Comparison between GSM-R coverage level and EM noise level in railway environment," in Proc. ITST, Lille, France, 2009, pp. 123−128.

[4] C. Steiner, A. Wittneben, "On the Interference Robustness of Ultra-Wideband Energy Detection Receivers," Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on, pp.721-726, 24-26 Sept. 2007.

[5] Mobile and personal communications committee of the Radio Advisory Board of Canada "Radio Advisory Board of Canada Useof jammer disabler devices for blocking PCS cellular and related services" available at: http:\\www.rabc.ottawa.on.calelfiles/01pub3.pdf

[6] M. R. Frater and M. Ryan, Electronic Warfare for the Digitized Battlefield. Norwood, MA: Artech House, 2001.pp 143-147.

[7] N.K. Mishra, "Development of GSM — 900 Mobile Jammer: An approach to overcome existing limitation of jammer," Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on , vol., no., pp.1-4, 15-19 Dec. 2009.

[8] V.K. Sambhe, , D.S. Kale, A. Wasule, N. Shikha, "Antenna for Mobile Phone Jammer," Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference on, pp.856-859, 16-18 July 2008.

[9] T. Braun, G. Carle,Y. Koucheryavy, V. Tsaoussids, "Wired/ Wireless Internet Communication," Third International Conference, WWIC 2005, Xanthi, Greece.

[10] R. O. Duda, P. E. Hart, and D. G. Stork, "Pattern Classification– 2nd ed". John Wiley & Sons, Inc, 2000.

[11] A. P. Dempster, N. M. Laird & D. B. Rubin, "Maximum Likelihood from Incomplete Data via the EM Algorithm Journal of the Royal Statistical Society," Series B, 1977, 39, 1-38.

[12] P. E. Greenwood and M. S. Nikulin, "A Guide to Chi-Squared Testing," John Wiley & Sons, New York, 1996.