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 3.4

"Assessment of the monitoring and detection solution: test report"

Submission date: November 2015

Deliverable on the assessment of the monitoring and detection solution
Date: 04/11/2015
Distribution: Public
Manager: IFSTTAR

Document details:

Title	**"Assessment of the monitoring and detection solution: test report"**
Workpackage	WP3
Date	04/11/2015
Participants to the R&D work	M. Heddebaut, S. Mili, Ch. Gransart, J. Rioult, Ch. Pinedo, G. Copin, J. P. Ghys, D. Sodoyer and V. Deniau
Responsible Partner	IFSTTAR
Document Code	SECRET-D34-A6
Version	A6
Status	Final version after final project review

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
A0	04/12/2014	M. Heddebaut	Initial skeleton of deliverable D3.4
A1	23/06/2015	M. Heddebaut, S. Mili, Ch. Gransart, J. Rioult	Initial version with all the scientific inputs
A2	30/06/2015	M. Heddebaut, S. Mili, Ch. Gransart, J. Rioult	First complete draft version
A3	18/09/2015	M. Heddebaut, J. Rioult	Add NetBox experiments and results – reorganize the deliverable structure
A4	02/10/2015	M. Heddebaut	Minor adjustments after circulation among WP3 and WP4 participants
A5 – final version	12/10/2015	M. Heddebaut	Modifications to the executive summary and to the general conclusion after peer reviewing by ALSTOM (Pierre Lambert). The peer review report is available separately.
A6 – final version after final project review	04/11/2015	M. Heddebaut	Modifications to the executive summary and to the final conclusion.

Table of content

List of figures

Executive summary

In previous WP3 - D3.1 to D3.3 deliverables, research activities and results related to SECRET WP3 “Monitoring the electromagnetic (EM) environment and detection of EM attacks” - Tasks 3.1 to 3.4 were presented. These tasks aim at developing sensors able to detect intentional electromagnetic interference (IEMI). Detecting IEMI is a first step in developing a resilient railway radio communication system as proposed in WP4. Therefore, electromagnetic measurements were performed in representative railway environments and their results were analyzed. Then, based on these in situ results, sensing techniques were developed considering additional IEMI. In this WP3 - Task 3.5 deliverable, these sensing methods are implemented using several hardware platforms. One particular objective of these implementations is to further evaluate the jamming detection potential of the studied techniques during demonstrations. These sensors were also developed to outperform an available commercial sensor whose latency time and too wide bandwidth were considered serious drawbacks for the development of the resilient architecture. During these demonstrations, the sensors provide the necessary input data to feed an Acquisition System (AS) connected to a Detection System (DS) so that the full system can decide if an electromagnetic attack really occurs and under which conditions. In this situation, the AS/DS followed by a reactive system launch an adequate reconfiguration of the radio communication system. After presenting a generic supervised method able to detect electromagnetic attacks operating in the GSM-R band, this deliverable focuses on the hardware implementations of the sensors and on their evaluations. Two complementary technical demonstrators are then selected and described. Their results are analyzed, the sensors performance are evaluated and the role of these sensors in the general reconfigurable radio architecture is evaluated.

1. Introduction

1.1. Purpose of the document

The purpose of this document is to present the work performed in SECRET WP3 - Task 3.5 towards a hardware implementation of the research and development work previously performed in WP3. For this purpose, different hardware platforms are successively considered and used. Therefore, the assessment of the SECRET project monitoring and detection solution can be performed, in particular through representative demonstrators.

This report particularly focuses on the detection of Intentional ElectroMagnetic Interference (IEMI) superimposed on a radio communication. D3.4 concentrates on the detection of the activity of limited power, in the order of 30 dBm, autonomous and portable jammers, operating at different frequency bands, between 800 MHz and 6 GHz and connected to low gain antennas. This jamming equipment could be switched on in the vicinity of radio receivers and jam the reception of information thus, preventing some operator’s phone and data exchanges. These exchanges are mandatory for the smooth operation of the transportation mode.

As soon as a detection sensor has sensed jamming conditions at its level, it sends alert data to a distant acquisition system. This alert information can also include some locally measured characteristics of the jammed signal. Similar data are also received by the acquisition system coming from several sensors distributed in the railway environment (train, station and infrastructure) to survey. Then, a Detection System (DS) connected to the acquisition system has the responsibility to decide if the radio communication and the whole system is effectively jammed or not. In such a case, the system deploys, at the physical layer and/or at higher communication layers, adapted countermeasures in order to cope with these interferences. In WP4, a particular reactive system based on a performant multipath communication system is specifically developed. Other possible countermeasures are also described in WP5.

In the following chapter 2, the jamming signals to be detected are analyzed considering existing commercial on the shelf (cots) wideband jammers.

In chapter 3, a test bench built using laboratory measuring equipment is assembled and a generic end-to-end detection method is analyzed. The main used scientific equipment in the test bench is an Keysight “PXA” or “MXA” signal analyzer covering the frequency range 3 Hz to 8.4 GHz, i.e. all the railway frequency bands of interest (see deliverable D3.1). The major advantage of using this expensive piece of equipment is that it is a real-time analyzer and that different complex detection pieces of software can be directly implemented and evaluated on it.

Chapter 4 presents the two Secret demonstrations that were performed respectively in April and September 2015. Since this deliverable D3.4 has a public status, it was decided not to propose a detailed analysis of possible techniques to disturb railway control command signals but rather than to consider realistic, but less sensitive demonstrations.

Chapter 5 is dedicated to our first full implementation and demonstration of the system. For the purpose of our proof of concept, we considered a generic case of study and we selected a video surveillance application whose video signal is transmitted over radio, up to a control center. A jammer can be operated in the vicinity of the receiver and jam the radio signals so that the video surveillance becomes no more effective. Considering the developments performed in WP4, an alternate radio path is used to cope with this problem and to work as a backup radio link. For this first demonstration, we selected WiFi and WiMAX radio communications operating at two frequency bands, i.e. 2.45 GHz and 5.6 GHz. This chapter continues by considering the relevant specifications of these two radio communication protocols and describes the upgrades performed to our preceding detection techniques (see deliverables D3.2 and D3.3) to be optimized in this new WiFi/WiMAX context. Then, the different sensors that were implemented for the demonstration are presented and evaluated separately. They provide the necessary 'real' sensors and output data to operate the AS and the whole reconfigurable radio system so that the global demonstrator can be assembled and evaluated in liaison with WP4 developments. Six sensors were used of which one is a commercial low-cost jamming signal sensor used as a reference. Since this sensor was not very well documented, it was also evaluated in laboratory. As indicated before, a real time signal analyzer was used as the heart of three different sensors. Since building operational sensing equipment with this state of the art, expensive measuring system, is not economically viable then, simplified sensors were also developed. They are still based on the above mentioned signal processing techniques but they are using simplified technical specifications. They are developed using commercial low-cost communication modules operating in dedicated GSM, GSM-R, WiFi... limited spectrum frequency bands. They are assembled to provide low-cost operational sensors that can also be directly interfaced with the AS. The chapter continues with a presentation of the complete sensor management system that enables to operate simultaneously the six sensors in their operating environment in order to evaluate their level of performance i.e. their capacity to detect low power jamming signal before they really affect the communication system, latency time… The continuation and end of the chapter are devoted to the demonstration results and to an analysis of them.

Chapter 6 focuses on our second demonstrator. It was selected in order to extend the scope of our initial demonstration. It uses on the one hand, a railway radio communication representative equipment, i.e. an ALSTOM NetBox and, on the other hand, a non-proprietary radio link i.e., a 3G radio communication associated to WiFi. Almost the same sensors and database as for the first demonstration were used. However, in the NetBox existing hardware equipment scenario, it was difficult to implement the original multipath communication system as it was done for the initial demonstration. Instead of that optimal configuration, a potentially less performant configuration was setup. Simple Evolutionary Algorithm for Multi-Objective Optimization (SeaMo) was implemented on a Linux based laptop. Seamo is used as a vertical handoff implementation for heterogeneous wireless networks. The testbed also comprises network elements that support HIP based mobility management for IPv4 as used by the 3G provider. Moreover, the tests were performed using the Secret WP3 sensors associated to a simplified local AS and DS. The DS delivers an information to the NetBox indicating that jamming conditions have appeared in the 3G or, alternatively, in the WiFi band. This incoming information had for consequence to switch the NetBox radio configuration from an initial radio link to the backup link i.e. 3G to WiFi or WiFi to 3G. This chapter particularly focuses on detailed timing measurements and analysis.

Chapter 7 concludes this deliverable. Bibliographical references are then provided.

1.2. Definitions and acronyms

	Meaning
AP	Access Point
AS	Acquisition System
AWGN	Additive White Gaussian Noise
BTS	Base Transceiver Station
CCA	Clear Channel Assessment
COTS	Commercial On The Shelf
DBPSK	Differential Binary Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DS	Detection System
DSSS	Direct Sequence Spread Spectrum
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
FHSS	Frequency Hopping Spread Spectrum
GD	Good Detection
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile communications
GSM-R	Global System for Mobile communications - Railways
GUI	Graphical User Interface
HAM	Health Attack Manager
HIP	Host Identity Protocol
HIPERLAN	High Performance Local Area Network
HSL	High Speed Line
IR	InfraRed
ISM	Industrial, Scientific and Medical
MIMO	Multiple-Input Multiple-Output
MPTCP	MultiPath TCP
MCM	Multipath Communication Manager
MS	Mobile Station
OFDM	Orthogonal Frequency-Division Multiplexing
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
SEAMO	Simple Evolutionary Algorithm for Multi-Objective Optimization
SJR	Signal-to-Jamming Ratio
SNR	Signal-to-Noise Ratio
TGV	Train to Grande Vitesse (High Speed Train)
VHO	Vertical Handoff
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

2. Jamming signals to be detected

2.1. Considered jammers

Different types of jamming devices exist. These are all illegal devices that cannot be sold or operated in most countries [1]. However, they can be easily found on the Internet. These devices are small and discreet [2]. Many of them use several independent frequency oscillators that sweep large frequency ranges quickly, in a few microseconds. Industrially, they can be easily derived from existing cell phone or nomadic devices hardware [3].

To present this initial generic detection method, we shall consider the specific case of the GSM-Railway (GSM-R) radio communication system [4]. This system is currently under deployment all over Europe and provides phone and data exchanges in many different railway operating environments i.e. in stations and depots, along the tracks, between trains and control centers…We shall develop a detection method derived from existing EMC tests using a template to define different zones of functioning. Although this work is initiated by a railway issue, GSM and GSM-R [4] are derived from a common communication protocol and existing jamming devices can, for some equipment, cover the contiguous frequency bands of both systems. The need to detect jamming signals may also be considered in other domains using 2G, 3G or 4G digital radio communication, especially for critical functions. We can notably mention the monitoring systems that automatically trigger cellular phone communications in case of detection of abnormal situations like malicious or unauthorized intrusion.

2.2. Jamming waveforms to be detected

Figure 1 shows a time-frequency representation of a signal generated by such a typical jammer. The measured levels are given in dBV and are indicative since the measurements were performed in conducted mode, by directly connecting the output of the jammer antenna to a -40 dB combiner. The 40 dB attenuated output was then connected to an oscilloscope 50 ohm port. The signal was measured with a 10 GS/s sampling and a sliding FFT was applied to obtain the displayed time-frequency representation. The representation covers a 50 μs duration and the 700 MHz to 1 GHz frequency range. This result confirms that the interference signal does not cover permanently the whole frequency band and that, consequently, the radiated power is shared in the whole swept frequency band. This particular jammer continuously scans a frequency band ranging from 840 MHz to 976 MHz, coming back every 8.20 microseconds on each channel. Therefore, both downlink and uplink frequencies of the GSM-R band are covered. Indeed, the jamming signal stays a very limited time in each 200 kHz wide GSM (-R) channel. The rest of the time, the jamming signal interference seems negligible in the frequency channel used for communication.

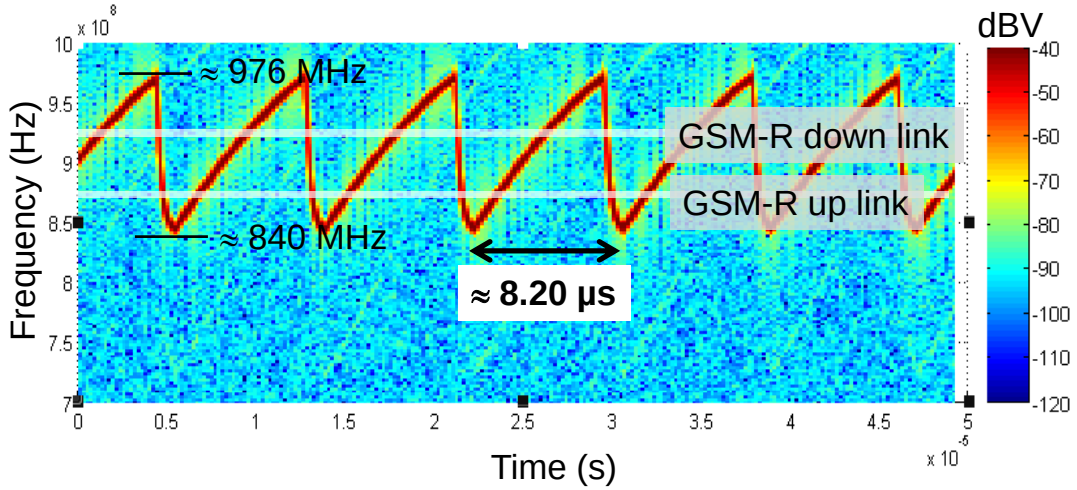


Fig. 1. Time frequency representation of a measured typical jamming signal.

Therefore, knowing that a GSM-R bit time duration is 3.7 μs, we could conclude that such jamming signals can affect about a third of the data bits. However, we do need to take into account the time constant of a 120 kHz input filter installed in the receiver chain, before the IQ signals demodulation. To consider this point, using this jammer, we measured the interference received by a spectrum analyzer set to zero span, centered on 923 MHz, a typical GSM-R channel, and using a 120 kHz resolution bandwidth. This resolution bandwidth was selected in order to be in a similar configuration to that of a GSM terminal. The measurement result are presented in figure 2.

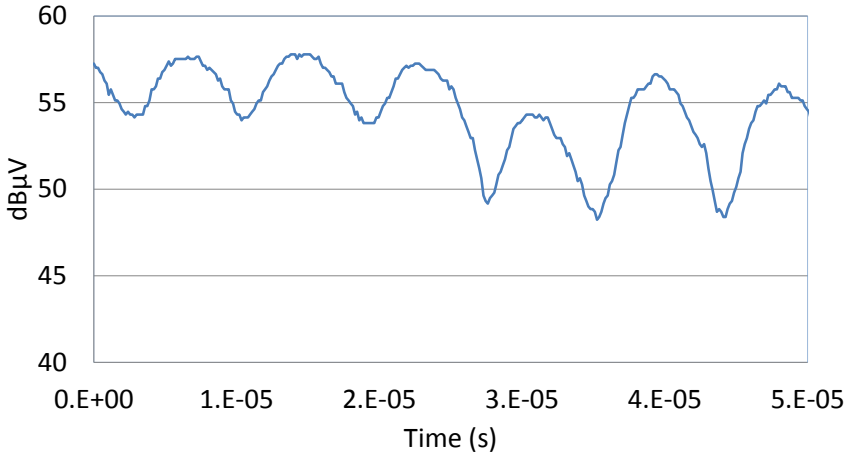


Fig. 2. Jamming signal measured in a 120 kHz resolution bandwidth at 923 MHz.

Considering the received interference, after filtering, figure 2 shows that using the filter, signal variation is reduced as compared to the previous results obtained in figure 1. We still notice the 8.2 µs time interval between consecutive maxima but the difference between the maximum and minimum values is now lower to 10 dB. Therefore, although the signal sweeps very fast, many bits of communication could be affected by the jamming signal.

Following these signal characteristics, we now present the laboratory test bench develop to detect jamming signals.

3. Generic method for detecting a GSM-R electromagnetic attack

3.1. Introduction

In this section, we shall present an end-to-end method which was initially developed to detect these jamming signals. In this section we shall consider the case of a GSM-R radio communication. Since jamming an operational GSM-R communication could have a severe impact on a real train operation, the test is operated in a laboratory controlled environment. Therefore, a local GSM-R communication is established between a GSM-R protocol emulator and a train GSM-R Mobile Station (MS). Then, the different steps of the detection method are analyzed.

3.1.1. Generating a local GSM-R communication

To generate a local GSM-R communication, we use a CMU GSM-R protocol emulator from Rohde & Schwarz associated to a GSM-R train mobile station (MS). They are operated in an anechoic chamber. The GSM-R emulator works as a local Base Transceiver Station (BTS) and handles the communication with the MS. Both BTS and MS are connected to external low gain antennas. Fig. 3 represents this part of the test bench. Data are continuously exchanged between MS and BTS.

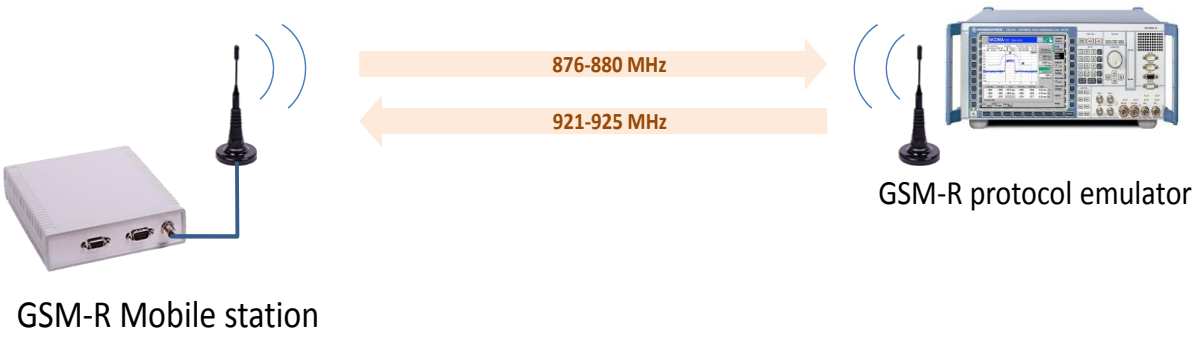


Fig. 3. Generating locally a GSM-R communication.

3.1.2. Generating a jamming signal

To generate jamming signals, we use either a local waveform generator, or a COTS wideband jammer. Figure 4 represents this equipment added to the test bench initially constituted of the GSM-R communication equipment alone.

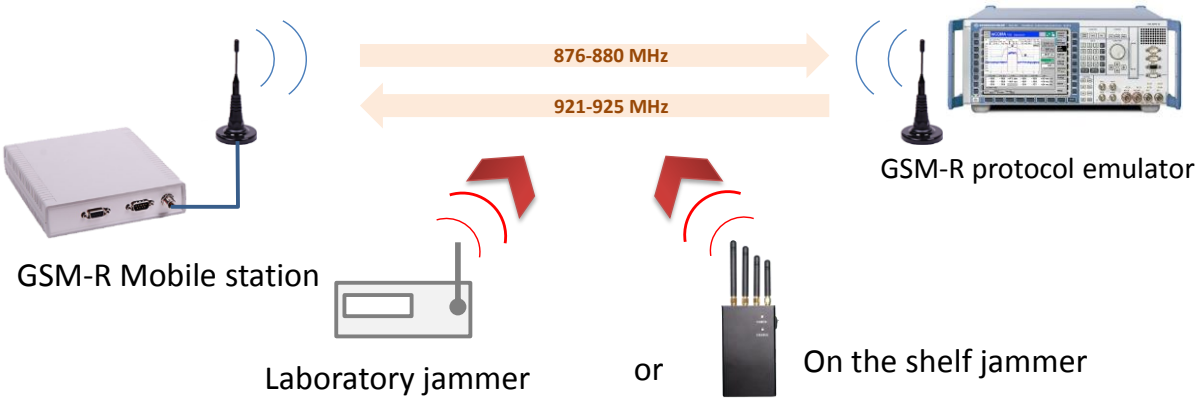


Fig. 4. GSM-R communication and jamming system.

3.1.3. Hardware detection system

The hardware detection element is composed of a real time signal analyzer (Keysight PXA-N9030A) in which various software jamming detection methods can be downloaded and executed. They correspond to different tested detection strategies. The analyzer is connected to an external antenna which receives both communication and jamming signals. This antenna is located in the vicinity of the GSM-R MS to receive similar radiofrequency signals to the MS. Thus, the complete test bench can be represented as in figure 5. An external computer is also used to manage the system, to store the data, and to transfer information to the distant acquisition system.

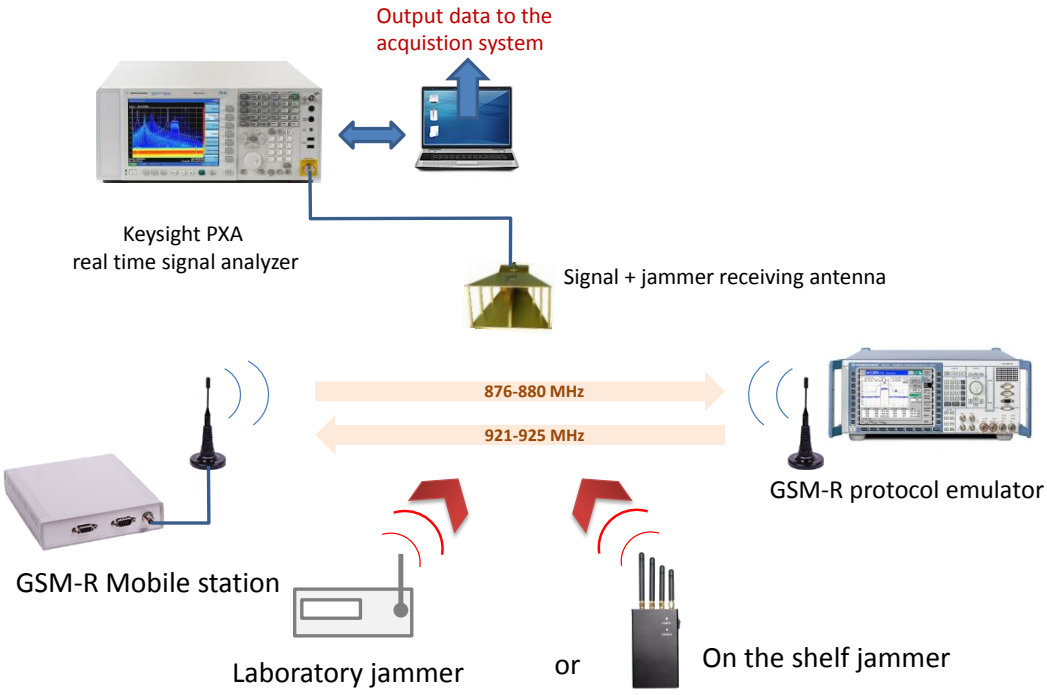


Fig. 5. Complete operational test bench.

3.2. Generic supervised detection method implementation

Anomaly detection consists in detecting unusual activity patterns in the observed data. Based on a supervised technique, our detection method aims to identify all signals away from a representation of the EM environment called ‘normal’ which corresponds to a typical radio activity in the observed

frequency band. Therefore, initial acquisitions are necessary to set up a learning phase in order to define the 'normal' EM environment in which the radio communication operates [5].

The detection method uses a descriptor [6]. In this method, the power spectral density (p.s.d.) is considered. Other descriptors can also be efficiently used like the Error Vector Magnitude, or the total radiofrequency energy present in a given bandwidth, for examples. Using the test bench, we propose to exemplify this methodology by presenting and analyzing the next four figures.

3.2.1. Learning phase

Figure 6 shows three different windows corresponding to the initial, learning phase of the method.

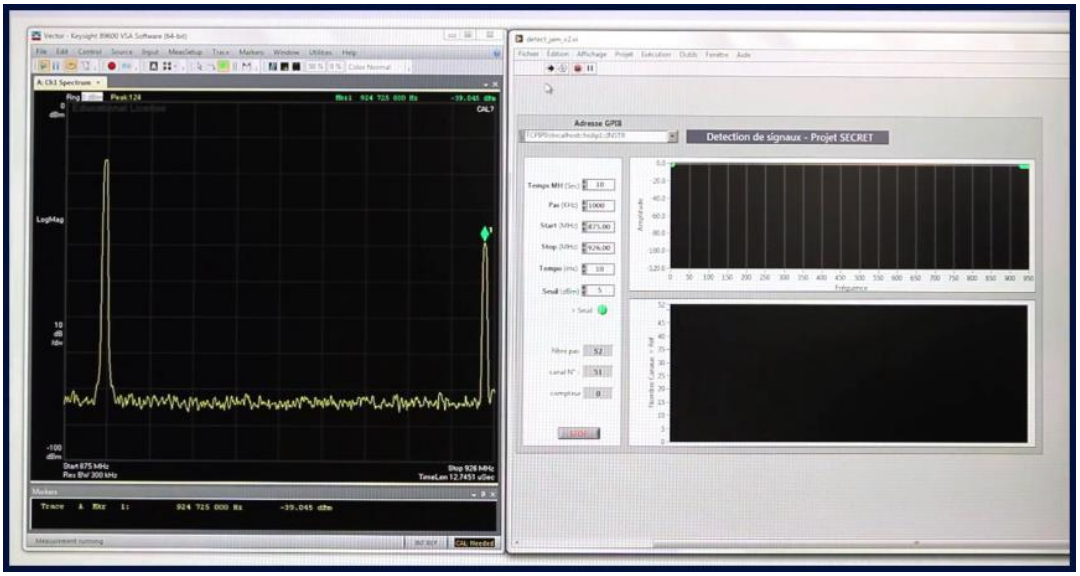


Fig. 6. Phase 1, learning a 'normal' environment.

A 'normal' environment is learnt during this period. The analyzer repeatedly scans a selected frequency band during a predefined amount of time. We progressively construct a template corresponding to all the appearing signals in the band of interest. We make the assumption that during this learning phase, 'normal' EM environments, without jamming signals, are observed. We consider the whole frequency band ranging between 876 MHz and 925 MHz therefore, including the 45 MHz guard band separating the uplink and downlink GSM-R radio channels (see figure 5).

In this figure 6, we notice two signals. On the left window, at the lower frequency, we observe the signals transmitted from the MS to the BTS. GSM-R data frames are only 576 μs long and can be seen only thanks to the real time analyzer used. In the upper frequency band, 45 MHz higher, we observe the data frames coming from the BTS to the MS. The relative received powers depend on the particular disposition of the different antennas and are not significant.

For this particular learning phase, we use a 'maxhold' function run for a predefined amount of time. The learning phase duration depends on the considered EM environment and on its complexity. After the scanning period is completed, a final template is computed by adding a predefined uniform gain to each of the measured frequency points. At the end of the learning phase, this final template is stored and will be displayed on the upper right-hand window of the next figures.

As a consequence, the threshold between 'normal' and 'jammed' condition is now delimited by this template. After this learning phase and this threshold determination, considering the p.s.d. descriptor used, the jamming detection phase can start. Future measurement results remaining below the template will be considered as 'normal' radio activity, and any signal above the template could be a potential jamming or interfering signal, detected as such, and sent to the acquisition system.

3.2.2. Normal conditions measurements

In phase 2 conditions, represented in figure 7, the real time analysis has started, the analyzer continuously scans the frequency band, looking for potential signals above the template; this previously computed template is represented on the right-hand upper window.

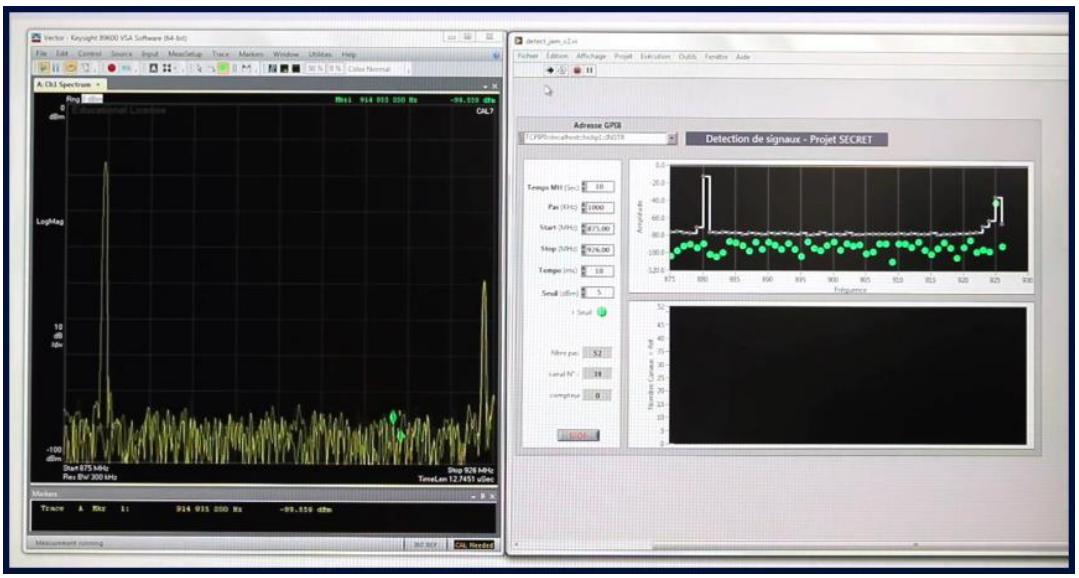


Fig. 7. Phase 2, real time analysis of the incoming signals.

In this figure 7, in the left-hand window, we obtain the almost real time measurement results generated by the signal analyzer. In the upper right-hand window, we show the template and the current p.s.d. values extracted from the signal analyzer over a predefined number of points. During this analysis, no jamming signal was applied. As a consequence, all the measurements are below the template.

3.2.3. Jammed conditions measurements

In phase 3, we now activate a COTS wideband jammer close to the MS. Its signals are superimposed on the communication channel and beyond. Fig. 8 presents the results corresponding to this phase.

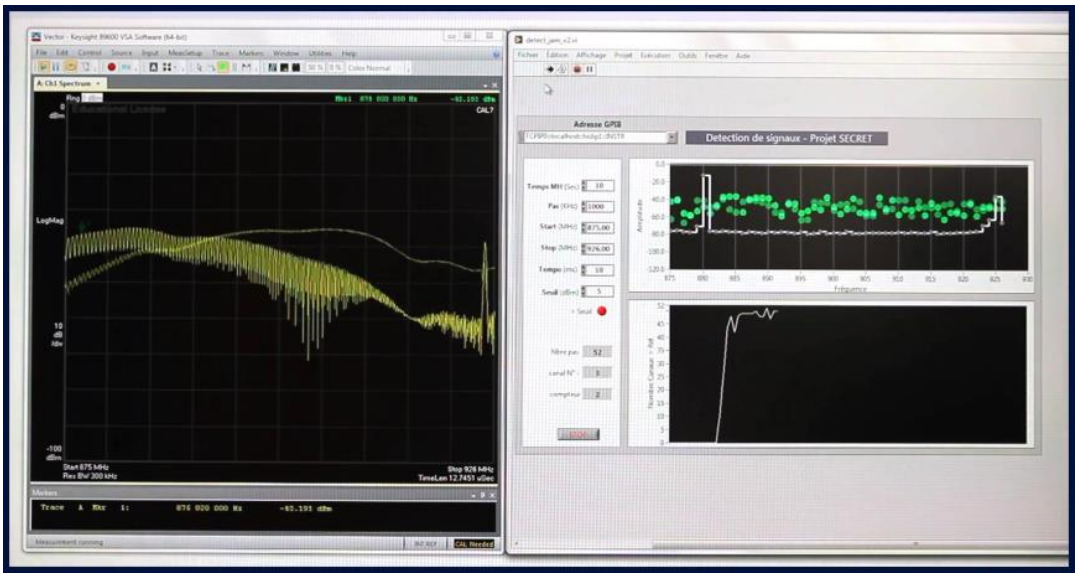


Fig. 8. Phase 3, detection of a jamming signal and extraction of relevant characteristics.

In the right-hand window, the wide band jamming signals characteristics are displayed. They refer to the results provided in figure 1. The figure 6 and figure 7 previously displayed BTS signal is also distinguishable. On the upper right-hand screen, we observe the corresponding computed learning phase template. In these particular jamming conditions, almost all the received p.s.d. measurements are above the template. In the lower right-hand window, we indicate the number of impacted GSM-R channels as a function of time.

Indeed, the jamming sensor quickly detects the overall number of jammed communication channels, the detected jamming levels above the threshold per channel, and also the jammed channels. As mentioned before, the sensor delivers its locally detected information to the acquisition system followed by the detection system which can then activate adequate countermeasures.

It is interesting to continue the analyzing process, up to the time the jamming signal is interrupted. This corresponds to a final phase 4. The corresponding results are presented in figure 9.

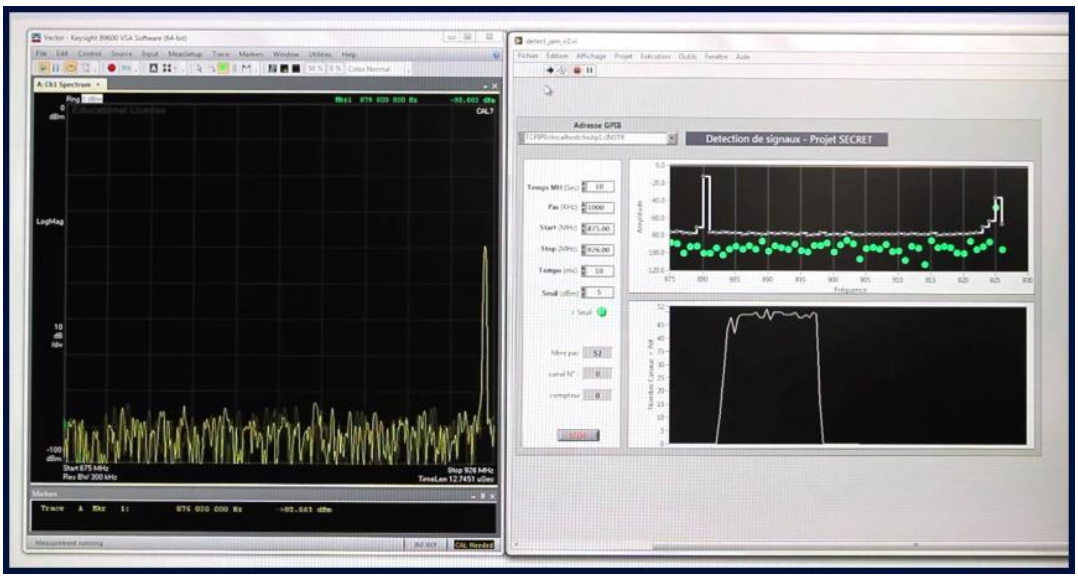


Fig. 9. Phase 4, the jamming signal is interrupted, the radio link is broken.

In the left-hand window of this figure 9, we observe that the jamming signal has been stopped. The downlink signal from the BTS to the MS still exists in the upper frequency band. However, in the lower part of the band, the uplink signal does not subsist anymore. Indeed, the radio link has been definitely blocked and interrupted by the jamming signal. Removing the intentional interference does not re-establish automatically the radio link. GSM-R is a connected mode. Therefore, both downlink and uplink communications were broken almost simultaneously although only one link was jammed, the MS received signal. In the upper right-hand window, all the signals are now back to 'normal' values below the template corresponding to 'normal conditions, and in the lower right-hand window, the number of impacted channels came back to zero.

3.3. Conclusion

After presenting this generic method, it is interesting to note that, except for the information recorded by the jamming sensor and sent to the acquisition system, there is no longer any easy way to detect that a jamming perturbation has been applied previously, against the radio communication system. Therefore, only an "unexpected" error is identified. Therefore, in the absence of jamming detection sensors, it could be difficult to clearly explain why the radio communication has been lost.

4. Secret demonstrations

As written in the introduction, since jamming real GSM-R signals on board a train or along the track could have intolerable impact on real train operation, the Secret demonstrations were oriented a different way.

Moreover, since this deliverable D3.4 has a public status, it was decided not to propose a detailed analysis of possible techniques to disturb railway control command signals.

Therefore, for the purpose of our proof of concept, we considered two generic cases of study. Firstly, we selected the case of a video surveillance whose video signal is transmitted over radio up to a control center. This case of study is derived from the monitoring systems that automatically trigger cellular phone communications in case of detection of abnormal situations like malicious or unauthorized intrusion. These systems can be inhibited using electromagnetic jammers. Secondly, we considered the case of a railway "netbox" equipment provided by Alstom. This product, designed for railway applications, provides wireless communication interface for all products embedded inside a rolling stock.

In both demonstrators, a jammer can be operated in the vicinity of the corresponding receivers and jammed the radio signals so that some communication functionalities become no more effective.

The two following chapters 6 and 7 present these two demonstrators and the results obtained.

5. Video surveillance demonstration

In our first video surveillance demonstrator, as developed in WP4, an alternate radio path is used as a countermeasure to the problem of jamming the primary radio link. In case sensors associated to the AS detect that the primary radio communication are possibly jammed then, the DS can decide that moving to the alternate radio path becomes necessary. In this case, the multipath communication manager (MCM) efficiently reorients the video flux to the alternate radio link and associated protocol.

Deliverables D4.4 and D4.5 present a detailed analysis of this MCM architecture.

For the purpose of the demonstration, we considered two different radio communications operating in two different radio bands. A WiFi link is used, running at 2.4 GHz and a WiMAX radio link operating in the 5 GHz band.

Figure 10 gives an overview of this scenario.

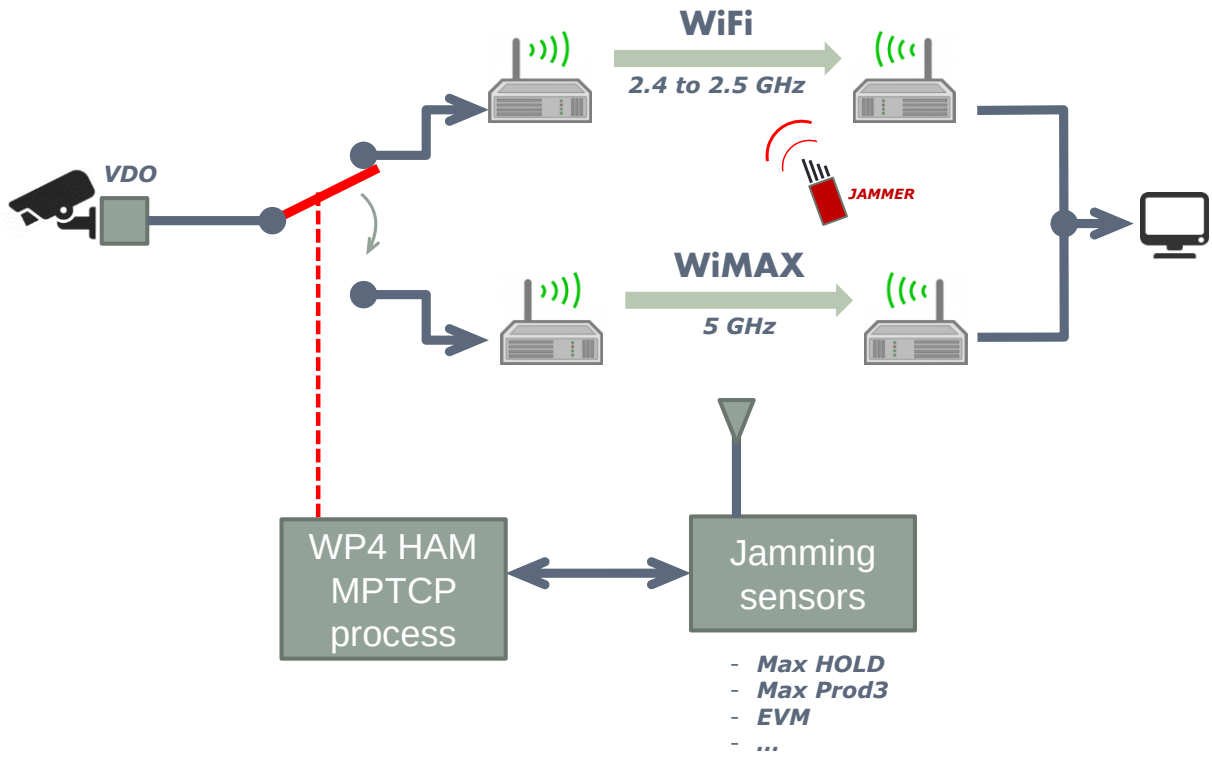


Fig. 10. Secret case study for the demonstration.

In deliverables D3.2 and D3.3, we have already explored two different techniques to detect jamming conditions. The first one relies on the analysis of the IQ signals used in any digital receiver, the second one performs spectral analysis. Let us now describe how we have optimized these methods to the specific cases of the WiFi and WiMAX radio protocols.

5.1. Detection process for WiFi/WiMAX communication

In deliverable D3.3, to identify the presence of a jammer, we have proposed to collect the I/Q information directly inside the existing equipment, at different stages along the receiving chain and to develop a specific signal processing to detect EM attacks. We selected and studied 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 exploited to evaluate quality parameters of a radio communication.

For the demonstration, this method has been refined to be adapted to the two WiFi and WiMAX

selected standards. Therefore, this document presents the detection methods dedicated to the different WiFi/WiMAX communication norms. Based on the EVM parameter, we shall study the evolution of the detection methods according to the different norms. Our system takes in consideration the evolution of the *EVM* in the time domain and in presence or in absence of jamming signals.

5.2. Introduction to the WiFi/WiMAX norms

The 802.11 group was initiated in 1990 and the standard IEEE 802.11 defining the WLAN networks was established in 1997. The standard defined three physical layers for the same MAC layer corresponding to three types 802.11 products [7].

IEEE 802.11 FHSS, uses the Frequency Hopping Spread Spectrum technique [8].
IEEE 802.11 DSSS, uses Direct Sequence Spread Spectrum [8].
IEEE 802.11 IR, uses infrared technique [8].

The IEEE 802.11 standard evolves over time and many improvements were made to the original standard. New physical layers have been added with IEEE 802.11b, IEEE 802.11a, IEEE 802.11g and IEEE 802.11 n [9].

IEEE 802.11b, also called WiFi is the improvement of IEEE 802.11 DSSS. Compatible with IEEE 802.11 DSSS, it uses the same ISM (Industrial, Scientific and Medical) band as the IEEE 802.11 standard but develops speeds up to 11 Mbit/s.

IEEE 802.11a or WiFi 5, different from DSSS and FHSS 802.11 and 802.11b standard, uses a new band, called U-NII (Unlicensed National Information Infrastructure) band of approximately 5 GHz to reach the speed of 54 Mbit/s.

IEEE 802.11g uses the ISM band with speeds up to 20 Mbit/s. This standard uses the OFDM waveform of the 802.11a standard, but remains compatible with 802.11b and IEEE 802.11 DSSS.

Finally, IEEE 802.11n the evolution of the 802.11g, incorporates MIMO (multiple-input and multiple-output) dimension [10].

5.2.1. Layer architecture

The IEEE 802.11 standard defines the first two layers of the OSI model, namely the physical layer and the data link layer (DLL), divided into two sub-layers, the LLC sub-layer (Logical Link Control) and MAC (Medium Access Control).

The following table 1 illustrates the architecture of the model proposed by the 802.11 working group compared to the OSI model [11].

OSI Layer 2 Data Link Layer	802.11 Logical Link Control (LLC)					
	802.11 Medium Access Control (MAC)					
OSI Layer 1 Physical Layer (PHY)	FHSS	DSSS	IR	Wi-Fi 802.11b	Wi-Fi 802.11g	Wi-Fi5 802.11a

Table 1: IEEE 802.11 layers.

The physical layer of the IEEE 802.11 standard is the interface between the MAC layer and the support for sending and receiving frames. Each physical layer for the 802.11 / a / b / g standard is divided in two sub-layers:

The PMD (Physical Medium Dependent), which manages the encoding of data and performs modulation.

The PLCP (Physical Layer Convergence Protocol) that inspects the media and provides a CCA (Clear Channel Assessment) to the MAC layer to report that the channel is free.

5.2.2. Physical layers

As indicated above, the original 802.11 standard defined three basic physical layers, FHSS, DSSS, IR, later three new physical layers were added, WiFi (with two variants within the 802.11b solution) and WiFi 5 (802.11a / g) [11]

5.2.2.1. FHSS (Frequency Hopping Spread Spectrum)

FHSS means a band spreading technique based on frequency hopping, in which the ISM 2.4 GHz band is divided into 79 channels bandwidth of 1 MHz each. To transmit data, the sender and receiver agree on a specific jumping sequence to be carried out on these 79 sub channels. The FHSS layer defines three sets of 26 sequences, totaling 78 sequences of possible jumps.
The transmission data requires jumping from one sub channel to another every 300 ms, in a predefined sequence. This hopping sequence is defined to minimize the collision probability between simultaneous transmissions. It is mandatory known by the receiver to recover data. This technique was previously used in military communications to secure their communications. Upon release of the ISM band in 1985, they also made free use of FHSS.
In this layer, the data is transmitted using a GMSK modulation between 1 and 2 Mbit/s. Its advantage is that it allows the possibility to simultaneously run 26 networks (corresponding to 26 sequences) in the same area, where each network uses a predefined sequence. Another advantage of FHSS is its resistance to the interference, such a system jumps every 300 ms from one channel to another on the whole band. If interference occurs on a limited portion of the ISM band (one or more channels), this technique can limit the impact of interference [11].

5.2.2.2. DSSS (Direct-Sequence Spread Spectrum)

As the FHSS, DSSS divides the ISM band in 14 channels of 20 MHz each. The transmission is done only on one given channel. The width of the ISM band being equal to 83.5 MHz, it is impossible to place 14 adjacent 20 MHz channels without overlap as shown in the following figure 1. Indeed, there can be a maximum of three 802.11 DSSS networks transmitting on the same cell without risk of interference.

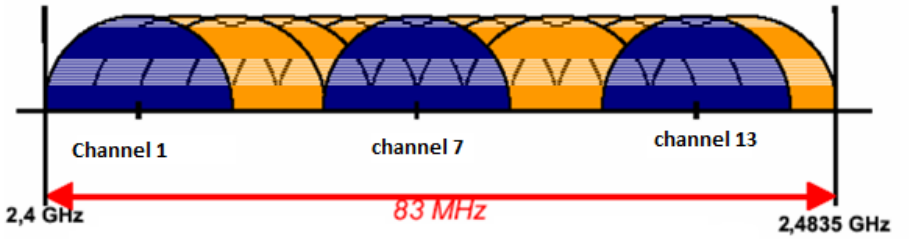


Fig. 11. Industrial Scientific and Medical band channel representation.

Spread spectrum is performed using a sequence of 11 chips, called Barker code (1-111-1111-1-1-1). Each bit of transmitted data is multiplied by this sequence of 11 chips. This approach strengthens the signal against narrowband interference. While noise affects only a part of the bandwidth, it will be possible to restore the signal to recover the information bits.

Two modulation schemes can be used: DBPSK (Differential Binary Phase Shift Keying), leading to a flow rate of 1 Mbit/s. DQPSK (Differential Quadrature Phase Shift Keying), leading to a flow rate of 2 Mbit/s [11].

5.2.2.3. IEEE 802.11b (WiFi)

Operating in the ISM band, the physical layer uses an extension of the DSSS, called HR / DSSS (High Rate DSSS). The HR / DSSS channels use the same system as the DSSS. The Wi-Fi networks and 802.11 DSSS are compatible and can communicate, but at rates of 802.11 DSSS, between 1 and 2 Mbit/s. The HR / DSSS have better spectral efficiency than the DSSS and provide two speeds: 5.5 Mbit/s or 11 Mbit/s.

5.2.2.4. WiFi (IEEE.802.11a)

Wi-Fi5 uses the U-NII band around 5 GHz. This band has a width of 300 MHz (instead of 83.5 MHz for the ISM band). The waveform used in IEEE 802.11a is similar to an ETSI standard called Hiperlan II. It provides theoretically high-speed of 54 Mbit/s. The 802.11a standard specifies 8 radio channels in the frequency band of 5 GHz. It uses an OFDM waveform based on an IFFT (Inverse Fourier Transform) of 64 carriers. To avoid the overflow on the band, only 52 among 64 carriers are used, the other carriers are set to zero. Among the 52 carriers used, 4 of them will be used to transmit known signals called pilot.

5.2.2.5. IEEE 802.11g

The IEEE 802.11g solution is a simple transposition of the IEEE 802.11a waveform from the U NII band to the ISM band. Except for this difference, the physical layer is identical to the one of IEEE 802.11a.

5.2.2.6. IEEE 802.11n

The latest IEEE 802.11 supports multiple-input multiple-output (MIMO) antennas and increases the maximum rate from 54 Mbps to 600 Mbps. 802.11n uses four spatial streams at a channel width of 40 MHz and operates on both the 2.4 GHz and the 5 GHz band.

5.2.2.7. WiMAX IEEE 802.16

WiMAX, also called IEEE 802.16 operates in frequency bands 2.5 GHz and 3.5 GHz, for which a license is required, and the free band of 5.6 GHz [12].
802.16 standard is based on orthogonal frequency division multiplexing (OFDM), and support modulations ranging from BPSK to 64 QAM. WiMAX supports both time-division duplex (TDD) and frequency-division duplex (FDD) modes [12].

5.2.3. *EVM* for IEEE 802.11 and IEEE 802.16 standards calculated by the VSA

EVM is commonly used to assess the quality of digital telecommunication signals. It expresses the difference between the expected symbol and the received symbol. The test instrumentation reconstructs the ideal signal based on the detected data and subtracts it from the actual signal to determine the error signal. At any single point in time, the error signal can be represented as a complex vector reaching from the ideal point in the I/Q plane, to actual location. Every chip has its own error vector. *EVM* is simply the RMS over 1000 chips. The ideal vector represents the theoretical instantaneous magnitude and phase of the carrier based on the known data stream [7][13].

For example the IEEE 802.11a/g and IEEE 802.16 standards use different OFDM modulation types (BPSK, QPSK, 16QAM, 64 QAM, etc.) that may be used in adjacent bursts. Even within one burst, more than one modulation format may be used since the four pilot subcarriers are always transmitted using BPSK. This motivates the use of normalization to calculate *EVM* easily and to enable direct comparison of *EVM* for a given average power level per symbol between modulation types [13].

EVM specification for the IEEE 802.11a/g, are then established according to the variation of the bit rate as shown in the table 2 [13][14][15].

Table 2: EVM evolution for IEEE 802.11g.

Data Rate (Mbit/sec)	Relative Constellation Error (dB)	EVM (% rms)
6	-5	56.2
9	-8	39.8
12	-10	21.6
18	-13	22.3
24	-16	15.8
36	-19	11.2
48	-22	7.9
54	-25	5.6

At the exception of the OFDM modulation, the EVM is calculated for the different IEEE norms using the following equation and that for the different modulation (BPSK, QPSK, 16 QAM, 64 QAM…).

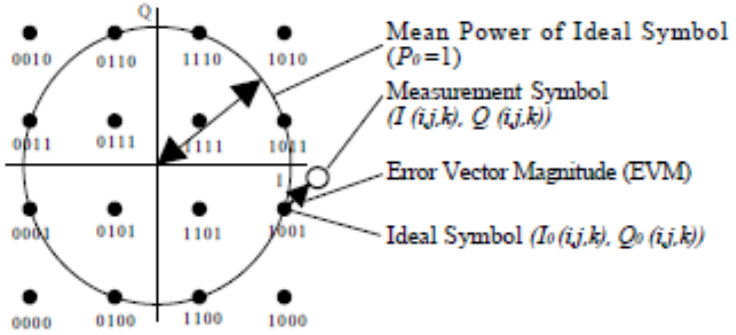


Fig. 12. Representation of 16 QAM modulation.

$$EVM_{rms} = \frac{\sum_{n=1}^{N_k}\left[\left|I(n)-I_0(n)\right|^2+\left|Q(n)-Q_0(n)\right|^2\right]}{P_0} \quad (1)$$

with:

N_k : number of symbols,

$I(n)$: I value for nth symbol,

$I_0(n)$: Ideal I value for nth symbol,

$Q(n)$: Q value for nth symbol,

$Q_0(n)$: Ideal Q value for nth symbol,

P_0 : mean power.

5.2.4. *EVM* demonstration

The jamming demonstration is carried out in a meeting room where WiFi and WiMAX equipment are deployed.

The spectrum analyzer (MXA) is used as an *EVM* sensor. The EVM process will then use information from the sensor, apply EVM treatment according to the protocol used and send binary detection information to the AS. The functional architecture of the process is described in the following figure 13. The EVM output is delivered to the acquisition system represented by the operator and the PC.

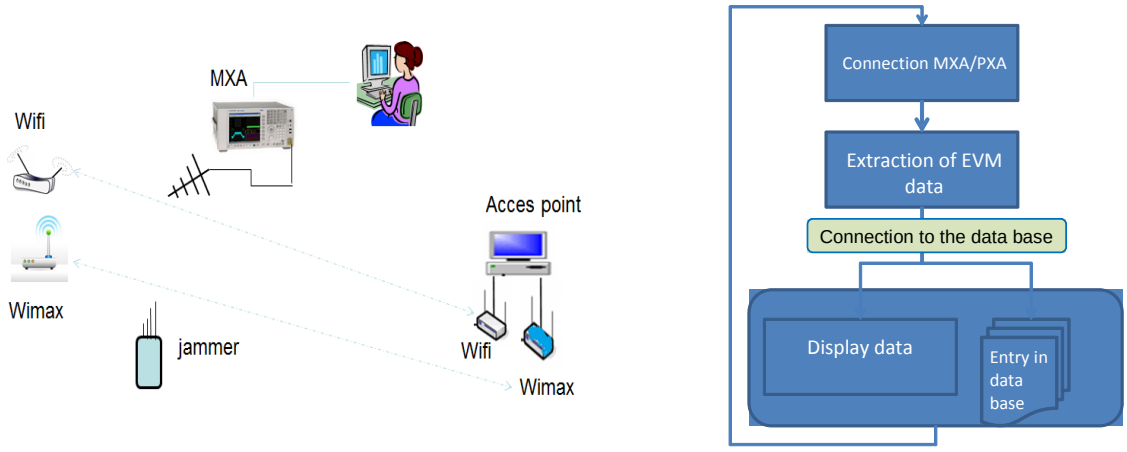


Fig. 13. EVM proposed architecture.

According to the system used (WiFi or WiMAX) the specific setup is selected to demodulate data frames. This setup needs to get information about the protocol (IEEE 802.11b,g, WIMAX IEEE 802.16), the center frequency of transmitted signal and the frequency band of the channel. According to this information the signal analyzer provides the different *EVM* values.

Transmitting a sensor information every 1 second to the AS, the processing is optimized to consider the *EVM* values received every second.

5.3. EVM processing for WiFi

The first step of the work studies the evolution of the *EVM* in 'normal' and 'disturbed' situations. According to the time evolution of this parameter, figure 14 shows how we then distinguish between 'normal' functioning and 'jammed' conditions.

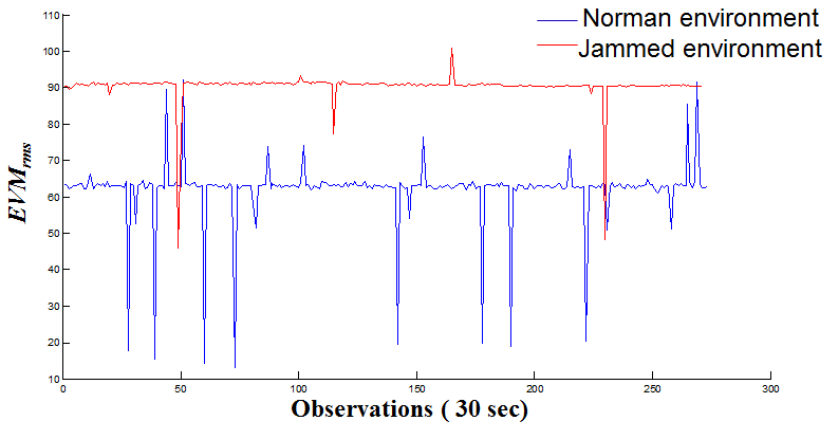


Fig. 14. *EVM* evolution during 30 seconds in normal and jammed situation.

We observe in figure 15 that the *EVM* follows a Normal distribution. We then apply the processing developed in deliverable 3.3 considering the GSM-R *EVM* process.

Then, the EVM sensor calculates a threshold from the normal situation which will represent the normal environment that the *EVMs* cannot exceed.

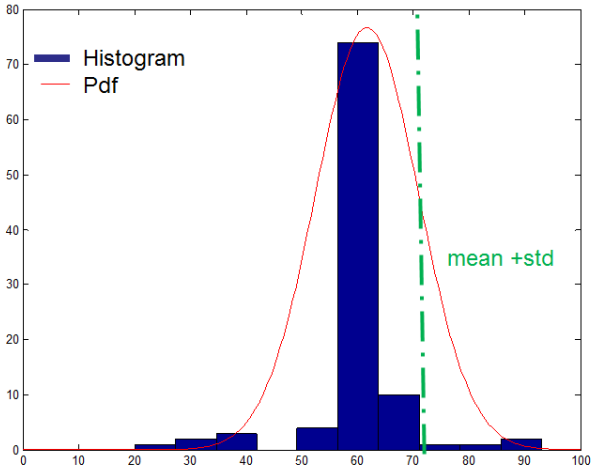


Fig. 15. *EVM* distribution and histogram for normal situation.

This process calculates the mean of the 1 sec *EVMs* and compares this value to the predefined threshold. If this value exceeds the threshold then, the process sends “1” as an output to the AS. In the other way, it sends “0” which means that there is no jamming signal detected locally.

During the experimentations, we operate a WiFi communication and we turn on and off the jammer located either close to the MS antenna or situated to a significant distance (15 m) from the MS antenna.

In all the tested conditions, as can be deduced from figure 16, the EVM measurement process was consistently able to detect jamming conditions emanating from both the COTS jammer and also from other locally generated wide band jamming waveforms.

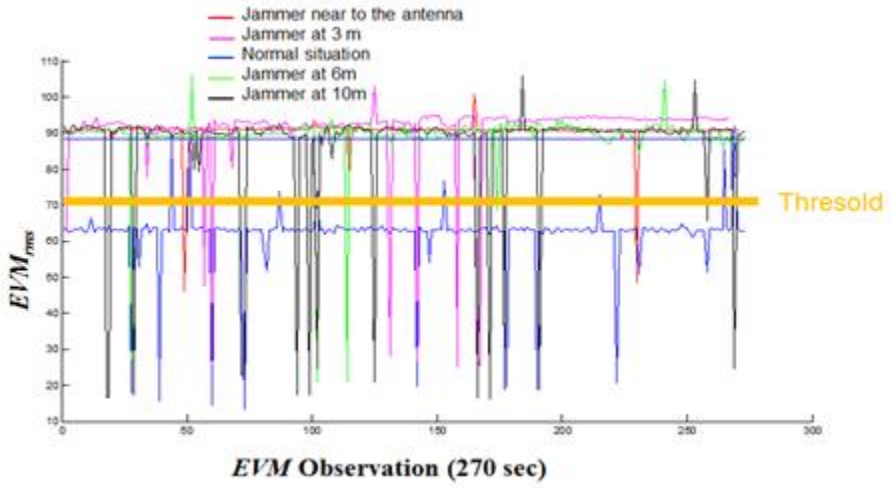


Fig. 16. EVM in normal condition and in presence of jammers switched on at different locations.

Moreover, also as observed in figure 16, the threshold level has a great importance to effectively determine the presence of jamming signals. This EVM process has the capability to detect low power jamming signals as they are far from the receiver antenna and/or using very low power Therefore, choosing an inadequate threshold can lead to some problems i.e. some false alarms or loss of detection can appear. To improve the detection process and to limit these false acceptance rate (FAR) a rule is made at the AS/DS level by making a decision of jamming if there are more than two successive positive detections. This solution provides a very sensitive sensor able to efficiently distinguish the presence of jamming at least after 2 seconds.

5.4. EVM processing for WiMAX

For the WiMAX case, we do not use directly EVM_{rms} but rather RCE (EVM). RCE (EVM) is the RMS level of the Error Vector Magnitude, averaged over all subcarriers (including pilot and data subcarriers) and all detected OFDMA symbols as presented in figure 17.

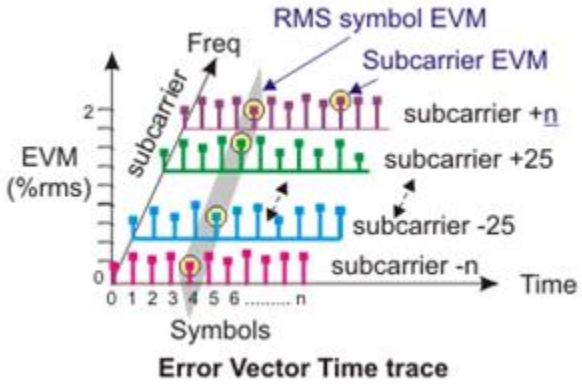


Fig. 17. EVM calculation for OFDM modulation.

These *EVM* values are calculated using the following equation after applying normalization [14][15].

$$EVM_{rms} = \frac{\left[\sum_{i=1}^{N_f}\left[\frac{\sum_{j=1}^{L_p}\left\{\sum_{k=1}^{52}\left[\left|I(i,j,k)-I_0(i,j,k)\right|^2+\left|Q(i,j,k)-Q_0(i,j,k)\right|^2\right]\right\}}{52*L_p*P_0}\right]\right]}{N_f}$$

where:
N_f: the number of analyzed frame,
L_p: number of symbol per frame,
$I(i,j,k)$: I value for kth subcarrier for jth symbol of ith frame,

I_0(i,*j*,*k*): Ideal I value *k*th subcarrier for *j*th symbol of *i*th frame,
Q(*i*,*j*,*k*): Q value for *k*th subcarrier for *j*th symbol of *i*th frame,
Q_0(i,*j*,*k*): Ideal Q value for *k*th subcarrier for *j*th symbol of *i*th frame,
P_0: mean power.

The *EVM* in dB is then calculated from this relation in equation:

$$EVM_{\mathrm{dB}} = 20*\log10\ (EVM_{rms}).$$

The *EVM* evaluate packets and frames for bursts with different modulation types. The ability to directly compare *EVM* for different modulation types is important since the IEEE standard specifies use of BPSK modulation for the four pilot subcarriers, while the 48 remaining data subcarriers may use a different modulation scheme.
In the same way as before, we study the time evolution of the RCE (*EVM*) in the normal situation to establish a decision rule. Due to this observation and those made under jamming conditions, we can define a new sensor able to recognize the presence of the jammer.

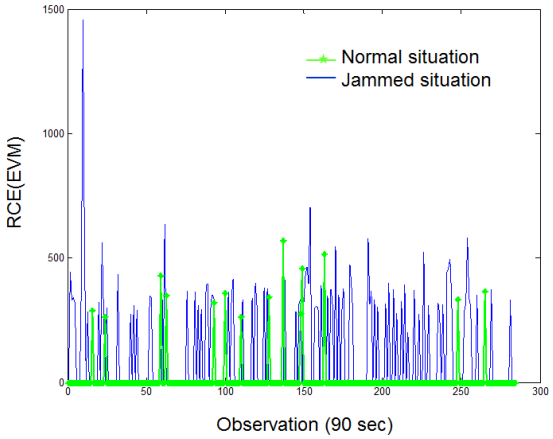


Fig. 18. RCE (EVM) evolution in normal and jammed environment.

As we can observe in figure 18, the decision process is different from what we used in WiFi. The RCE (EVM) evolution according to time presents a particularity. RCE (EVM) values equals to zero over a long period of time, this can due to the perfect demodulation and/or to the impossibility of the system to extract data. In the other way when jamming is present, the signal analyzer delivers a consecutive high values of RCE (EVM). According to this assumption and to the result presented in figure 19, we tried to establish a decision rule taking in account these successive rows of zero.

By calculating the total sum of the RCE (EVM) values during one second we can demonstrate the increasing level of RCE (EVM).

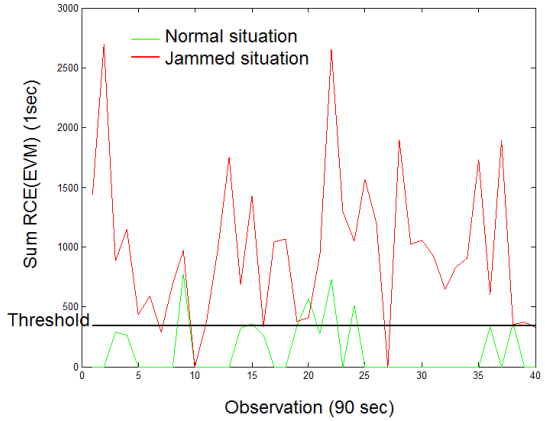
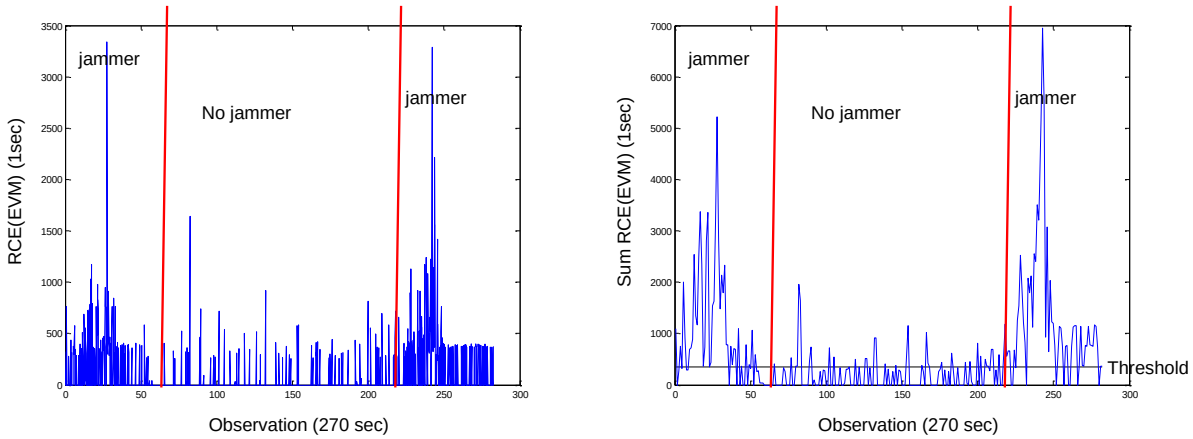


Fig. 19. One second total sum of RCE(*EVM*) for normal and jammed situation.

This new reasoning allows as the possibility to make an easier difference between normal and jammed situation as presented in figure 19. In this situation, using this new parameters, we defined a threshold able to detect the jammers. We still can observe some false alarms that can be avoided by moving the decision to more restrictive conditions. Finally, if more than two successive samples are

over the threshold then, we decide that we are in presence of a jamming condition. This has increased the total decision time to 3 seconds.



a b

Fig. 20. WiMAX demonstration a: RCE (EVM) evolution, b: sum of RCE (EVM).

Initial tests were performed by setting up a WiMAX communication. We turned on a COTS jammer operating at different output powers and we tried to detect the presence of these jamming signals by sending an output data (0 or 1) to the AS. Considering the RCE (EVM) process we were able to detect the presence of jammers. Figure 20 illustrates the evolution of the RCE (EVM) over time. We observe the normal situation and we distinguish the successive appearance and disappearance of the jamming signal.

5.5. Conclusion

Considering the *EVM* parameters for WiFi and WiMAX communication, after this optimization phase, we are now able to carry out a sensitive sensor able to identify the presence of jammers in a minimum delay of 3 seconds using our test setup.

5.6. Jamming sensors developed for monitoring and detection

5.6.1. Secret jamming sensors

Six different jamming sensors associating different hardware and signal processing were simultaneously tested during the demonstration using a common setup.

The maxhold method that was initially detailed in the presentation of the generic detection and monitoring method one of the used jamming sensor for the demonstration.

One commercially available sensor was specifically bought for the demonstration. Its role was to serve as a reference. It constitutes an additional sensor used for the demonstration.

The four remaining sensors were internally developed, starting from the results obtained in WP3 and tested during this demonstration.

The following section presents the commercial sensor and these four Secret developed sensors.

5.6.2. Commercial sensor

A commercially available jamming sensor was selected to be used as a reference for the other sensors developed in the Secret project. It is a moderate cost equipment (200 €) covering GPS, WiFi, GSM, 3G, Bluetooth, RFID and GSM bands. It is said to be high sensitivity and using fuzzy logic. The detection range is indicated to be up 20 m from the jammer. Figure 21 presents this commercial jamming sensor.

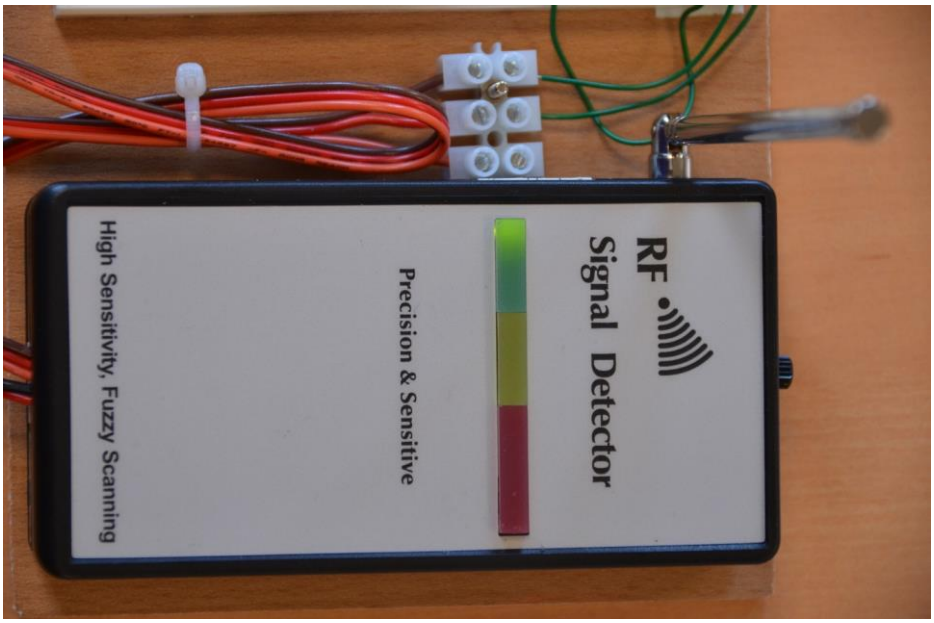


Fig. 21. View of the reference commercial jamming sensor.

As shown in this figure 21, an internal antenna is provided and the equipment is externally DC power supplied.

A single 0/1 output signal is delivered by the equipment.

The manufacturer provided documentation indicates that, within 10 s of the presence of a jamming signal operated in the detection area of the equipment, then, the output signal switches from 0 to 1.

To evaluate the performances of this sensor, we have measured its performances in an anechoic chamber, i.e. in presence of a calibrated CW study signal working as a steady jammer. The commercial sensor is installed on the table and a transmitter and associated antenna is used to illuminate the sensor over a wide frequency band. Figure 22 shows this installation.

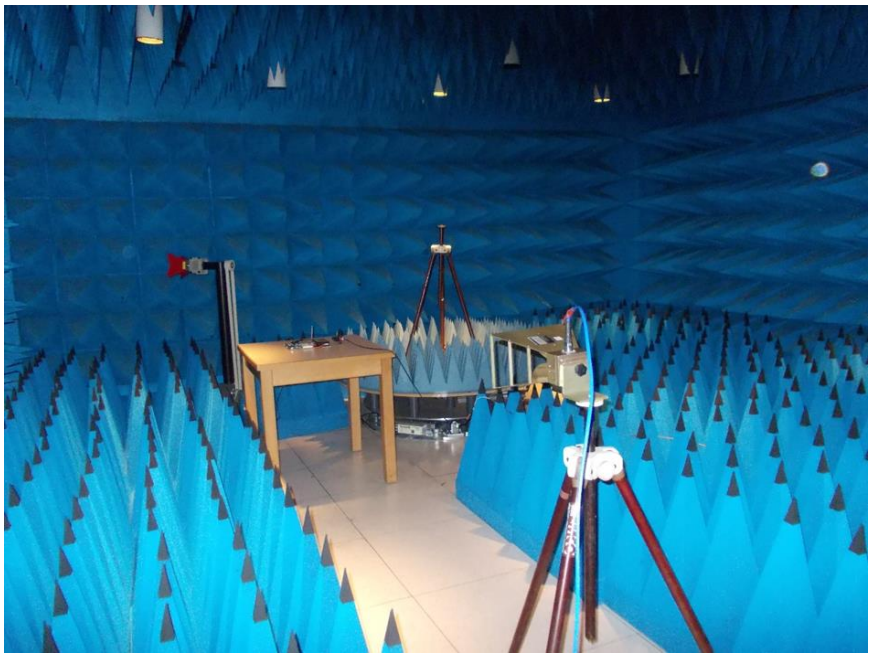


Fig. 22. Commercial equipment evaluated in an anechoic chamber.

We obtain the results presented in figure 23.

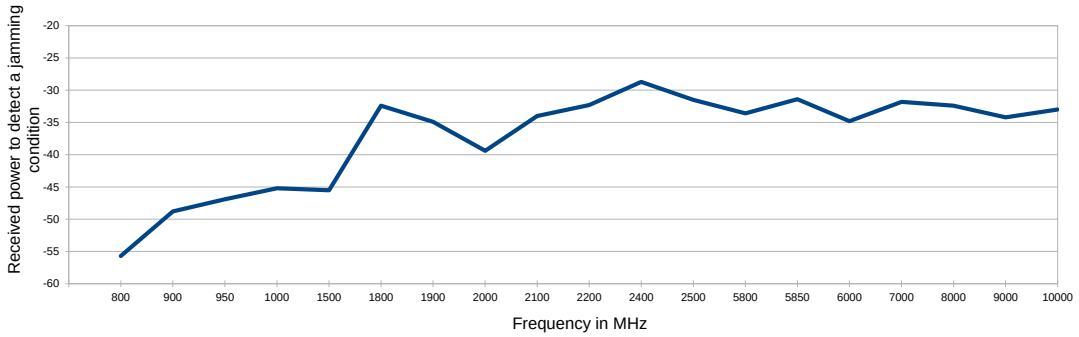


Fig. 23. Sensitivity vs. frequency of the commercial sensor.

A steady CW signal operated for 10 seconds or more effectively trigs the commercial sensor as soon as it reaches, at the sensor location, a power of -55 dBm at 800 MHz and -35 dBm at 6 GHz.

Therefore, the commercial sensor has a very large bandwidth covering from GSM-R to WiMAX frequencies, and more.

However, this sensor does not really discriminate between the useful communication signal and a jamming signal. Then, false detection can easily occur. Moreover, its sensitivity is low.

5.6.3. Secret IQ jamming detection method

5.6.3.1. Introduction

The IQ quadratic signals jamming detection method was developed and presented in the WP3 D3.2 deliverable. In a previous section of this deliverable, we have presented how this method is adapted and refined considering WiFi and WiMAX radio protocols. In this section, we now present the specific Graphical User Interfaces (GUI) developed to visualize the results, during the demonstrations.

5.6.3.2. Graphical user interface

This interface considers the methods developed for jamming detection on the GSM-R communication and then refined for WiFi and WiMAX.

It uses the *IQ* representation from the receiver. Based on the preliminary study using the EVM descriptor, the GUI requires a reference data to detect the jamming. It works on the principle of the following figure 24 chart.

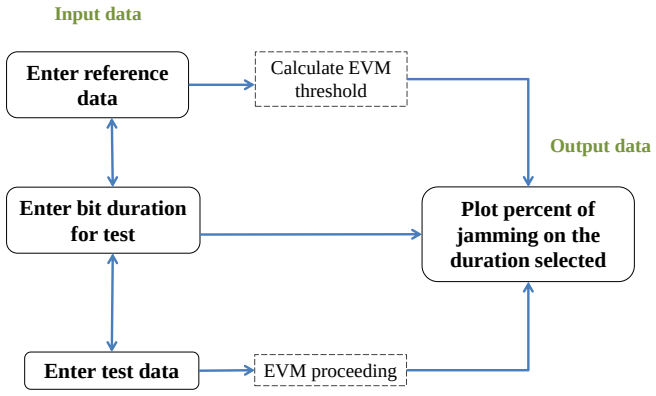


Fig. 24. EVM flow chart.

5.6.3.3. *EVM* method

The error vector magnitude (EVM) parameter commonly used to assess the quality of modulation for communication systems is selected as a descriptor to detect the presence of jamming. The EVM is extracted from the receiver and used for the test. As shown in figure 25 and knowing that the EVM follows a Gaussian distribution, the assumption was to test if the EVM values follow the Gaussian distribution taken as reference from the normal data.

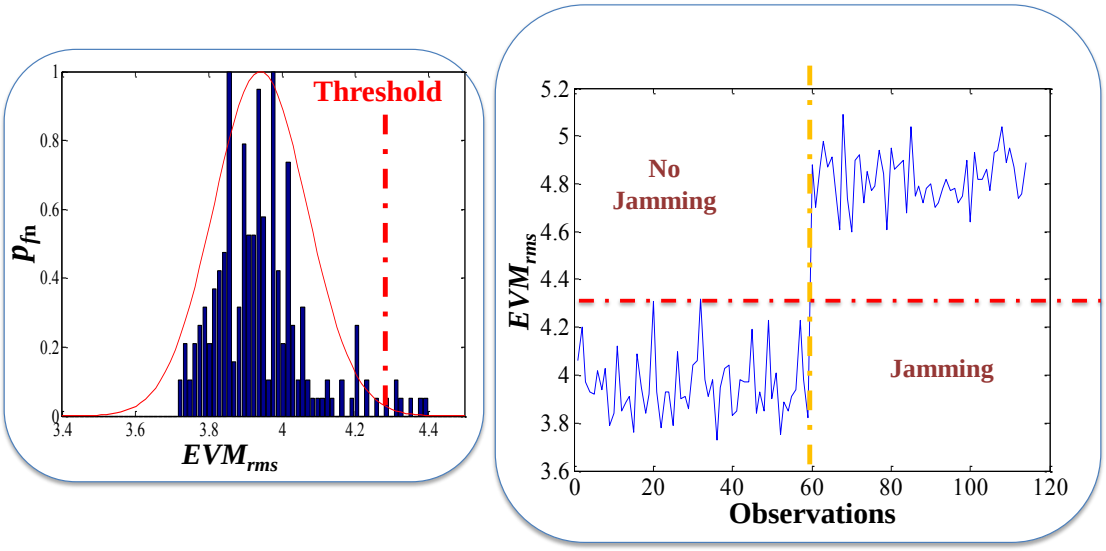


Fig. 25. EVM representation.

To avoid false alarms, the tests are done on a longer period (8 successive bursts). The interface takes in account all these constraints and parameters. We start by loading a reference data which is used to calculate the threshold, a second parameter is then introduced corresponding to the period duration of tests. It is set to 8 bursts as a predefined value. Other values can be selected during the tests. Then, the guide evaluates the test data and print the percent of jammed data contained on the period selected. If we obtain a final value of more than 20 % then, we consider that we are in a jammed situation.

5.6.3.4. EVM GUI

The interface, presented in figure 26, accepts a .txt file for the data of EVM references and EVM test. There is also an input window to select the length of the sliding window on which the calculation is made. Output interface gives us the percentage of EVM values in the sliding window that is outside the acceptable threshold.

Window 1
Enter the file reference

Window 2
Enter the length of the sliding window

Window 3
Enter the file for test

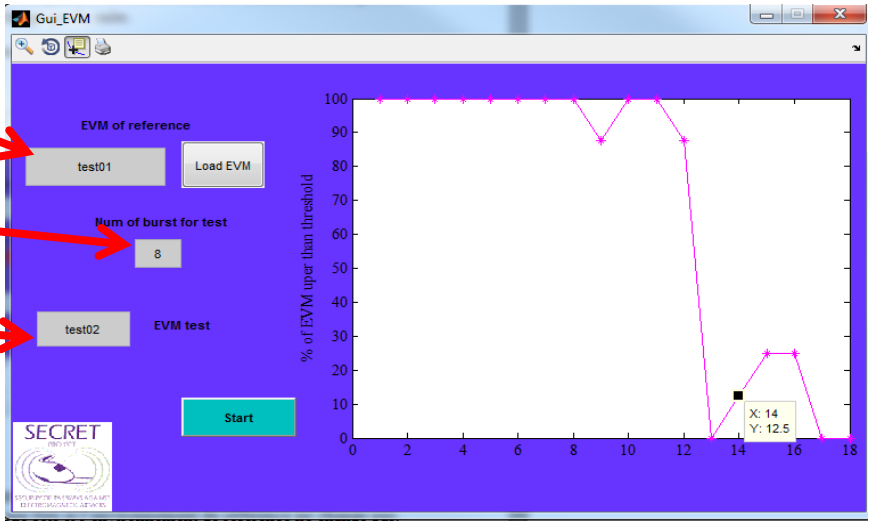


Fig. 26. EVM graphical user interface view.

The button ‘Load EVM’ loads the file reference written on the window 1 and calculates the EVM threshold. This action is imperatively done at the beginning of the tests. However, it is not necessary to reload the reference except in the case of changes in the radioelectric environment.

From the reference data:

$$\mu_{\mathrm{EVM}} = E\left[EVM\right] \approx \frac{1}{N}\sum_{\mathrm{n=1}}^{\mathrm{N}} EVM\,(t) \quad (1)$$

$$\sigma^2_{\mathrm{EVM}} = E\left[EVM^{\,2}\right] \approx \frac{1}{N}\sum_{\mathrm{n=1}}^{\mathrm{N}} EVM^{\,2}(t) \quad (2)$$

$$EVM_{\,threshold} \approx \mu_{EVM} + 3\sigma_{\mathrm{EVM}} \quad (3)$$

The button ‘start’ loads the test file. Then, we calculate from the sliding window and from the $EVM_{threshold}$ the percent of data upper over the selected threshold.

Data delivered by the GUI at the end of the process can be directly used by the AS/DS to proceed.

5.6.4. Detection of attacks in spectral space

The spectral analysis detection method constitutes the second method developed and presented in the WP3, D3.3 and D3.3 deliverables. We briefly recall this method and then present the specific GUI that was developed to operate the demonstrator.

The detection consists in determining whether each new observed spectrum belongs or not to a stochastic process defined by a generative model estimated forward with 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.

This principle is illustrated in figure 27. The power spectral density is recorded in the GSM downlink frequency band, over a span of 100 MHz. This particular measurement was performed in a railway station.

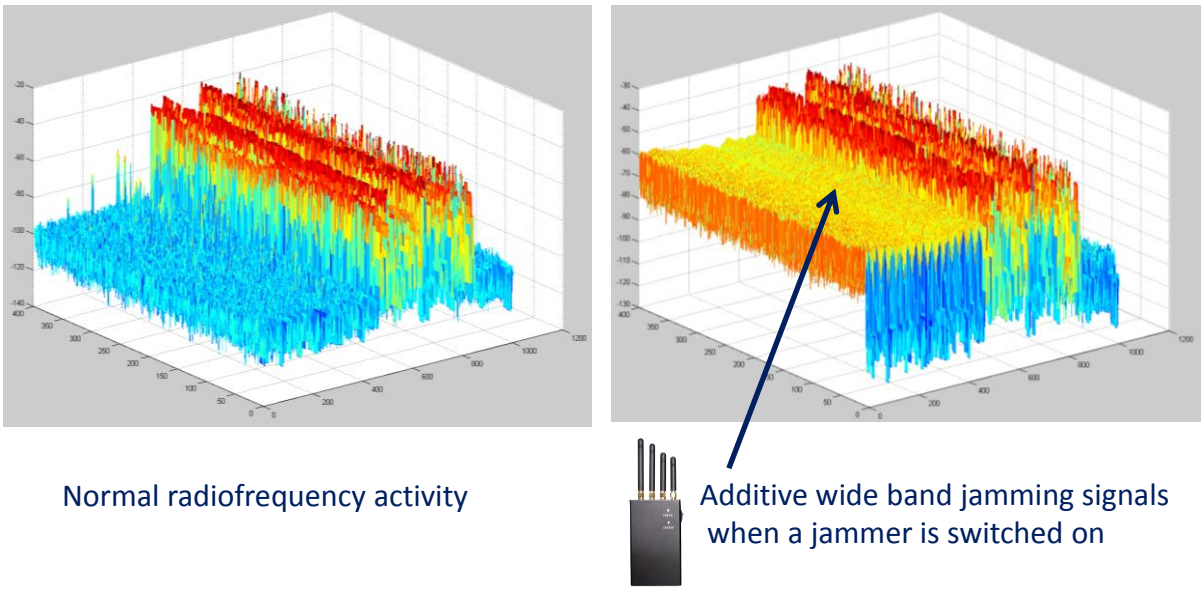


Fig. 27. Illustration of the spectral space detection method.

On the left side of figure 27, a ‘normal’ radio activity is recorded in the station. On the right side of the figure, a jammer is switched on. It modifies the received power spectral density. This difference is used to detect the electromagnetic attack.

This method is developed in liaison with our real time signal analysers (MXA and PXA).

5.6.5. MGM method

The MGM method is based on the study of the frequency distributions of the signals received by the antenna. The power spectral density (p.s.d) used as descriptor is recorded for the different states of the communication as presented in figure 28. The p.s.d between 850 MHz and 1 GHz are presented for the communication and different jamming devices.

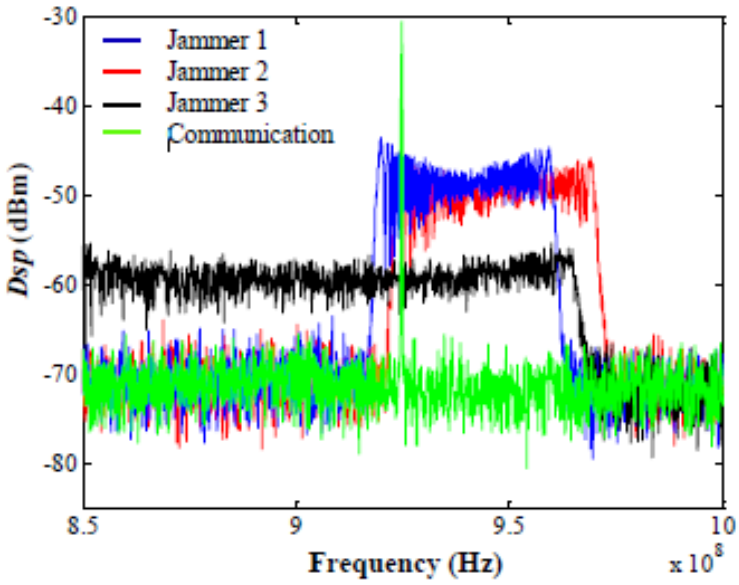


Fig. 28. Spectrum representation for communication and jammers.

The process considers a supervised classification method, using a statistical model (multi Gaussian) for each frequency of the spectrum. Different models are established during the learning phase for both the 'normal' conditions and 'jammed' conditions. In our case different models of 'attacked' conditions are defined using different jammers. Then, the detection process considers the Bayesian rules to calculate the matching fit for the different models.

5.6.5.1. MGM GUI

The associated GUI is represented in figure 29.

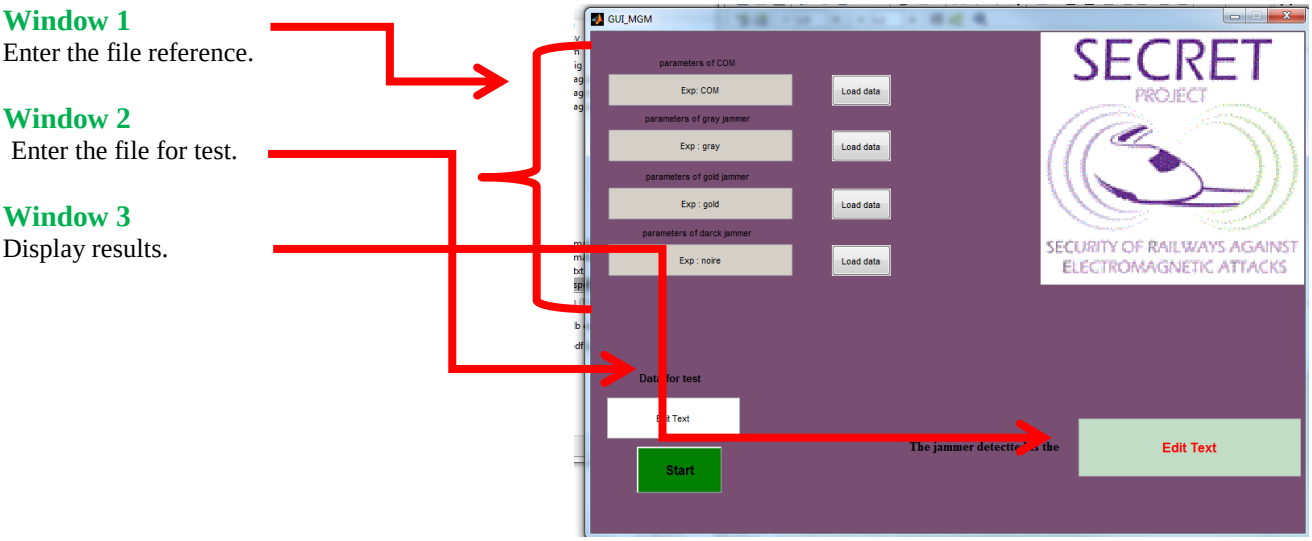


Fig. 29. MGM graphical user interface view.

The developed interface permits to load a reference file and then a data test file. The "Start" button loads the test file so that it is not necessary to load every time the reference environment. At the beginning of the analysis, if a jamming condition is detected, then a warning window appear to inform

that a jamming situation is detected. Then, closing this window reactivates the system to detect which type of interference is present. This information is displayed in window 3.

5.6.6. Dedicated Secret jamming sensors

5.6.6.1. Developing a prototype hardware

The two previous EVM and spectral analysis methods were implemented for the demonstration as scientific outputs of the theoretical development performed in previous WP3 steps. They used an expensive scientific equipment, a real time signal analyzer, to test our algorithms.

To develop detection jammer prototypes comparable in cost to the reference commercial jamming sensor, additional Secret dedicated jamming sensors were assembled. In this prototyping phase, they are constructed using commercially available modules. Figure 31 presents such a GSM module assembly.

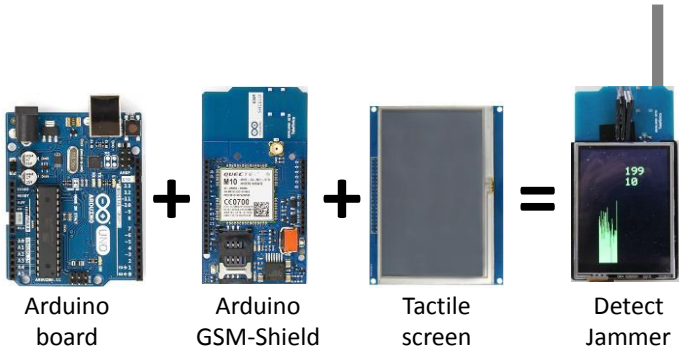


Fig. 30. Jamming sensor prototypes.

An Arduino™ GSM and a WiFi-shield boards are used. The GSM board has the capability to scan the cell phone bands and to extract data which reflect the p.s.d. values per channel. An additional Arduino™ board is used to get some local computation resources to implement the processing method and to also transmit the locally generated data to the distant acquisition system. A tactile display managed to locally visualize the results and to configure the sensor. As seen in figure 30, we finally obtain a three-layer, compact and low-cost sensor. Of course, this sensor is no more real time, but it still has the capability to scan 5 channels per second and also to easily implement different simplified processing techniques.

5.6.6.2. Secret spectral space signal processing

As presented previously, the used descriptor is the p.s.d. value and we make the assumption than no jamming signal exist during the learning phase. During this phase, the prototype sensor continuously scans the different channels of the band of interest and extracts the corresponding received p.s.d. values that are measured per channel. To simplify and accelerate the local processing, we add up the successive p.s.d. values measured during each scan to obtain a global value representing the 'normal' activity in the band. At the end of the learning phase, we determine the maximum of these stored values, select it and add a constant level to determine a final threshold. This constant level is necessary to limit false alarms.

During the measurements, any further scan resulting in a global p.s.d. value over this threshold will be declared as corresponding to a potentially jammed situation. We call this method the Max Prod process.

The jamming detection phase is then launched and the prototype sensor continuously scans the band, looking for jamming conditions and in this case, supplementary p.s.d. in the band. Jamming signals are applied.

5.6.6.3. Preliminary test

Before using this prototype sensor in the demonstration, preliminary tests were performed. We built the test bench presented in figure 31.

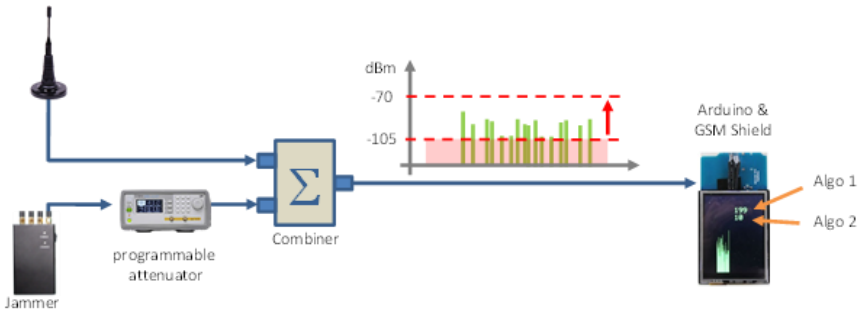


Fig. 31. Dedicated jamming sensor test bench.

2G signals locally received by an antenna are directed to a circulator/coupler. 2G signals were received at power levels in the range -50 dBm to -80 dBm. The noise floor of the GSM-shield board is -115 dBm. Via a programmable attenuator, the jammer output signal is also coupled to the prototype sensor. We measure the minimum necessary jamming p.s.d. to be effectively detected. Using different wide band jammers, this method has successfully and consistently detected wideband jammers at p.s.d. values of -76 dBm, a much better value than the measured sensitivity of the commercial sensor tested previously. As soon as the threshold was correctly set, we obtained a very low false alarm rate. As the sensor is run for extended periods of time, we found useful to re-launch a learning phase to reinitialize the process and re compute the 'normal' activity value. During this particular sensor learning phase, the electromagnetic surveillance relies on the other sensors.

5.6.6.4. WiFi shield scan for available networks processing

As mentioned before, another Secret prototype equipment was also assembled to support a different signal processing, dedicated to WiFi.

For this method, we make the assumption that at least one WiFi network is operational in the test area.

This method corresponds to specific commands implemented on the WiFi shield equipment. Our used command scans repetitively for available WiFi networks using the WiFi shield. It does not actually connect to any network, so no encryption scheme is specified.

If a jammer is active in the WiFi band then, no network will be operational and the list of available networks will be empty. Therefore, we indirectly detect that a jammer is operated.

5.6.7. Conclusion

Two low-cost Secret prototype equipment were developed that will be used for the demonstration. Because of the available computation resources of the prototype, the first one implements a basic version of the spectral space method scanning for the energies available in the different communication channels. The second one uses a command directly available on the receiver looking for channel availability.

5.7. Coupling the sensors to the acquisition system

Different equipment were used and assembled to realize the proof of concept demonstration.

Two laboratory real time analyzers (PXA and MXA) Keysight equipment were used for the real time acquisition of radio frequency signals.

Two « Secret » laboratory developed jamming sensors were also experimented

One commercially bought low–cost jamming sensor was working as a reference.

All these acquisition and processing equipment were interfaced with personal computers (PC) and connected to the same local area network using Ethernet links as represented in figure 32.

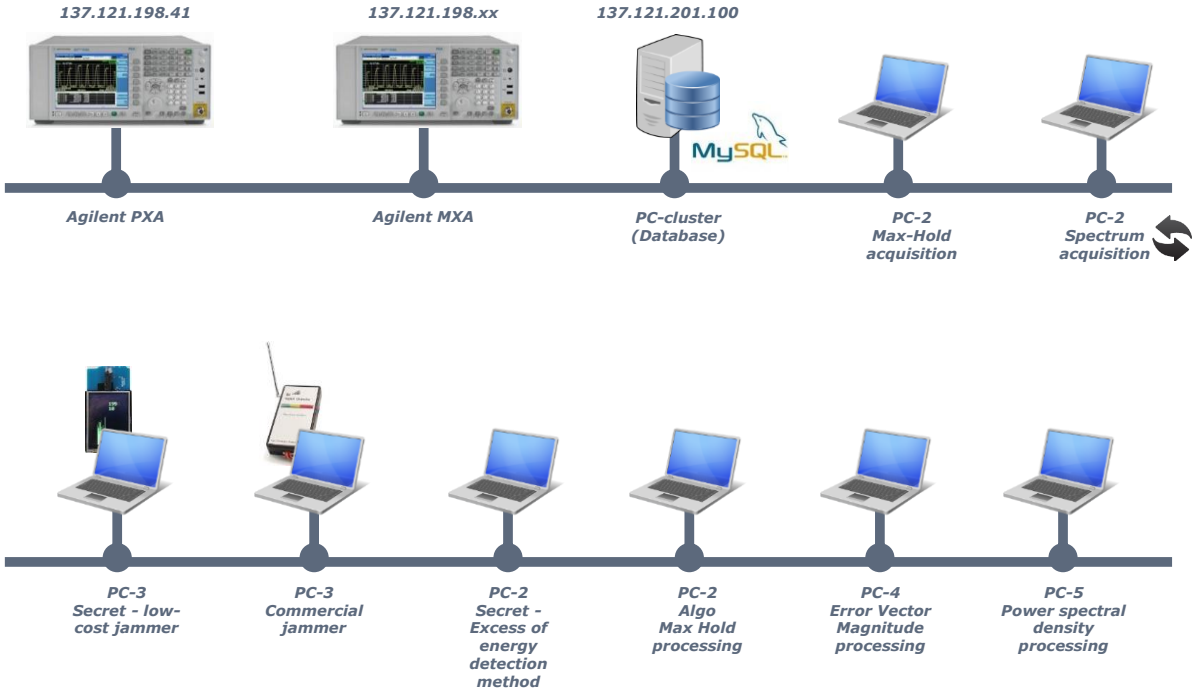


Fig. 32. Used equipment connected to the local network.

Moreover, a MySQL database was also setup. This database is used as a single means to write and read all the necessary information requested or provided by the different sensors and, to deliver the sensors outputs to the Acquisition System. This database was running on a high speed local computation cluster to accelerate the process.

The following common operating mode was defined for all the sensors:

- Step one: Acquiring data, this is performed externally by the PXA and MXA analyzers. The analyzers write periodically their output raw data in the database. The considered raw data was the power spectral densities measured in the selected frequency range and the measured Error Vector Magnitude in a communication channel.

- Step 2: Reading and processing the data. The sensors and associated PCs read the relevant data from the database. The signal processing algorithms are run on the corresponding PC and the results are written in the database.

- For those sensors that do not need external raw data (Secret low-cost jammer, excess of energy sensor, commercial sensor), their results are periodically written in the database to be used by the Acquisition System.

- Through the database, the AS has simultaneously access to all the sensor outputs.

The whole process is continuously run and refresh approximately every second.

An example of this first step of the process is detailed in the following figure 33 for the maxhold algorithm run on the PXA signal analyzer and detailed in the first section of this report.

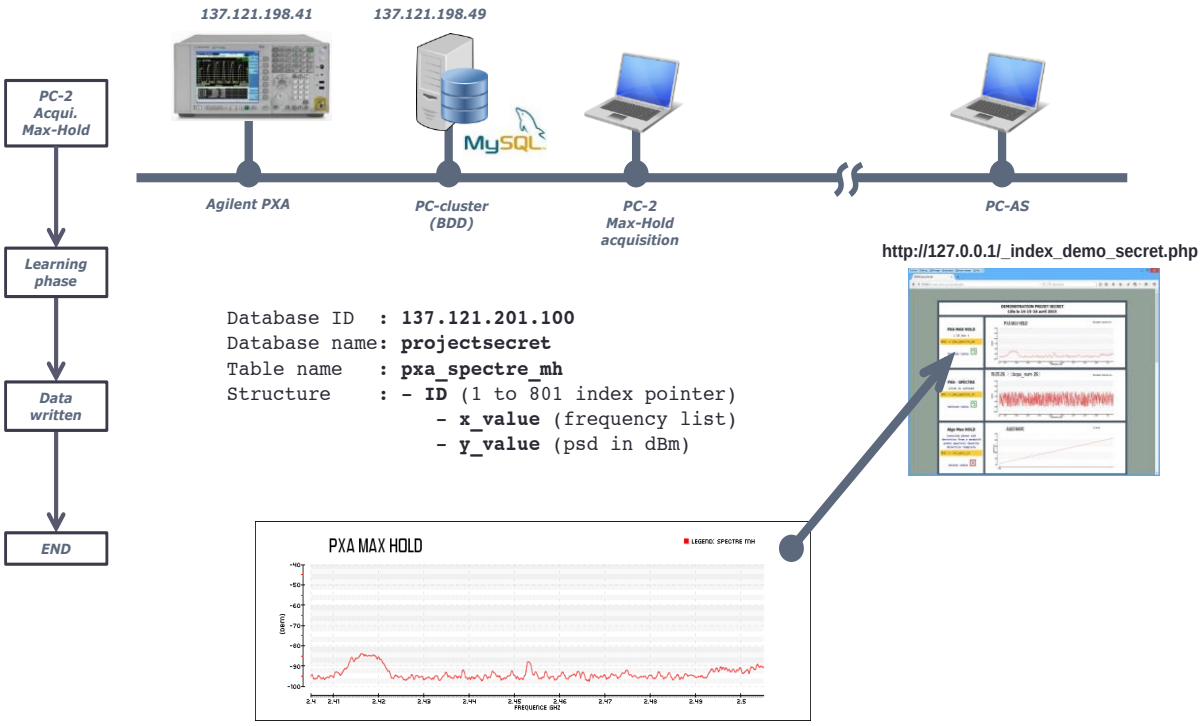


Fig. 33. Raw data acquisition and transfer to the database.

In this example, the PXA real time analyzer continuously writes, in the database, the received power spectral densities values measured to the selected frequency range.

Figure 34 presents the second step of the process.

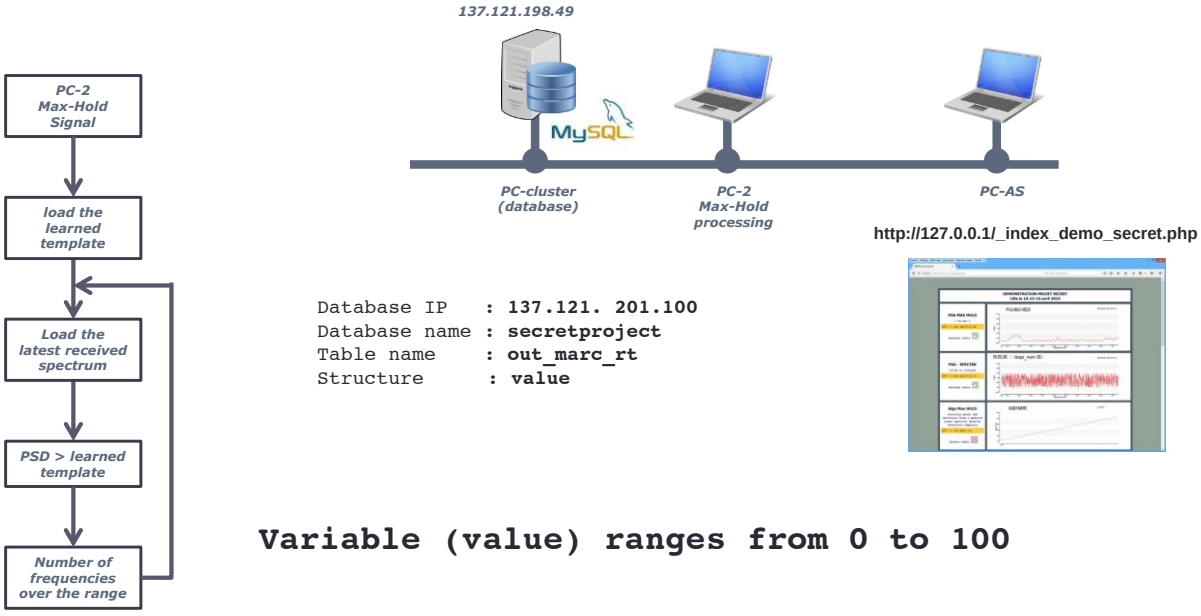


Fig. 34. Processing phase and result.

In this second step, PC_2 is operating the dedicated maxhold signal processing. PC_2 reads continuously, via the local network, in the database, the latest 801 p.s.d. values previously delivered and written by the PXA. Then, the learning phase starts for a predefined amount of time, a few tens of seconds in our case. During this amount of time, PC-2 determines a maxhold template corresponding to the maximum received p.s.d. at each frequency. At the end of the learning phase, the computed template is written in the database. We consider that no jamming is present during the learning phase.

Then, PC_2 continues reading, in the database, the latest data coming from the PXA and compares it to the template. If, for some frequencies, the current psd values for some frequencies exceed the one recorded in the template, then these frequencies are declared potentially jammed and their overall number is written in the database as the result of the maxhold detection algorithm. This information will be used by the AS reading another time the database.
In the case of a wideband jammer occupying all the scanned channels, the provided result is normalized to 100. On the contrary, 0 means that currently no psd exceeds the template or, that no radio channel is currently detected jammed.

The other sensors and associated data processing are operated the same way.

Using this methodology, our six different sensors can been operated simultaneously during the proof of concept demonstrations and have the capability to deliver almost simultaneously their output data to the AS.

5.7.1. Acquisition System and Detection System

Two versions of the AS were developed: one using the database and a second one using a real-time message queuing middleware. Whatever the technology used, after getting the current state of the sensors, a decision making algorithm is used next to evaluate the current wireless environment and determine of the equipment is under attack or not. In case of attack, the Acquisition System informs the Health Attack Manager (see deliverable D4.1) to develop a resistive response to the attack.

5.7.2. Acquisition System using a database

The AS that used the database fetches the current value of all the sensors each second. Next, the AS applies the decision making algorithm to evaluate the threat.

5.7.3. Acquisition System using a middleware

The AS using a middleware is described into deliverable D4.2 (Final specification of the dynamic protection system). The data coming from the sensors are transported using the message format shown in section D4.2 – 4.2.2.2.

For all kinds of sensor, the description of the data transported is the same and follows this syntax:

```
package SECRET_Acquisition is

--
-- Generic Message see Livrable D4.2
--
      ...

    --
    -- Example a data transmitted by the middleware (MaxHold sensor)
    --
    type Max_Hold is
        State : Current_State;
        Value : Integer; -- Sensor current value between [0..100]
    end Max_Hold;

end SECRET_Acquisition;
```

The Decision making algorithm is executed into the AS_Sink process.

5.7.4. Decision making algorithm

The decision making algorithm takes the values generated from the different algorithms and decides if the situation is correct or if there is a jamming condition. For all the developed methods, we present the decision logic. Next, we make a sum of all the algorithms that have reacted. The highest value we

have, the better jamming detection is obtained.

5.7.4.1. Algorithm Max Hold

For this algorithm, we are using a sliding window of two seconds. If the value given by the sensor is greater than 50 during at least two seconds then, we consider being are under attack.

```
//
//          Max Hold
//
            if (previous.outMaxHold.value > 50 &&
                current.outMaxHold.value > 50)
            {
                  result = true;
                  System.out.print(" MaxHold ");
                  nbSensors = nbSensors + 1;
            }else{
                  System.out.print(" -------- ");
            }
```

5.7.4.2. Algorithm EVM

For this algorithm, we are using a sliding window of three seconds. If the value given by the sensor is equal to 100 all the time then, we consider being under attack.

```
//
// EVM
//

            if (secondPrevious.outEVM.value == 100 &&
                previous.outEVM.value == 100 &&
                current.outEVM.value == 100)
            {
                  System.out.print(" EVM ");
                  result = true;
                  nbSensors = nbSensors + 1;
            }else{
                  System.out.print(" --- ");
            }
```

5.7.4.3. Algorithm Max Prod

For this algorithm, we are using a sliding window of two seconds. If the value given by the sensor is greater than 70 during two at least seconds then, we consider being are under attack.

```
//
// MaxProd
//
            if (previous.outMaxProd.value > 70 &&
               current.outMaxProd.value > 70)
            {
                  result = true;
                  System.out.print(" MaxProd ");
                  nbSensors = nbSensors + 1;
            }else{
                  System.out.print(" ------- ");
            }
```

5.7.4.4. Algorithm WiFi Secret Arduino

We consider being are under attack if the current value of the sensor is equal to 100. That means that no SSID is available.

```
//
// Arduino
//
            if (current.outArduino.value == 100)
            {
                  result = true;
                  System.out.print(" Arduino ");
                  nbSensors = nbSensors + 1;
            }else{
                  System.out.print(" ------- ");
            }
```

5.7.4.5. Algorithm spectral space or Bayesian

For this algorithm, we are using a sliding window of two seconds. If the value given by the sensor is greater than 70 all the time then, we consider being are under attack.

```
//
// Bayesian
//
            if (previous.outBayesian.value > 70 &&
                current.outBayesian.value > 70)
            {
                  result = true;
                  System.out.print(" Bayesian ");
                  nbSensors = nbSensors + 1;
            }else{
                  System.out.print(" -------- ");
            }
```

5.7.4.6. Algorithm commercial product

We consider being are under attack if the current value of the sensor is equal to 100. The startup time for this equipment is 10 seconds, so this equipment is not qualified as real-time. Moreover, this sensor reacts as soon as there is some radio traffic whatever the frequency used. So this algorithm is just used as a confirmation of an attack already detected by at least one of the above methods. This sensor can generate false positive in case of there is some traffic on a particular frequency but which is not the one that we are using.

```
//
// Commercial product
//
            if (current.outSwitch.value == 100)
            {
                  if (result != true)
                  {
                        falsePositiveSwitch = true;
                  }else{
                        positiveSwitch = true;
                  }
                  System.out.print(" Switch ");
                  // nbSensors = nbSensors + 1;
            }else{
                  System.out.print(" ------ ");
            }
```

The following table 2 presents an example of the trace of the execution of the detection system. In this trace, the EVM method detects first the jammer; the next second, the maxhold algorithm detects also the jammer. Few seconds later, the commercial product confirms that there is a jammer operating in the vicinity.

seconds	MaxHold	MaxProd	EVM	Arduino	Bayesian	Switch	MaxHold	MaxProd	EVM	Arduino	Bayesian	Switch
1	7	0	0	0	0	0	0	------	---	------	-------	-----
2	7	0	0	0	0	0	0	------	---	------	-------	-----
3	7	0	0	0	0	0	0	------	---	------	-------	-----
4	9	0	0	0	0	0	0	------	---	------	-------	-----
5	45	0	0	0	6	0	0	------	---	------	-------	-----
6	21	0	0	0	47	0	0	------	---	------	-------	-----
7	6	0	0	0	32	0	0	------	---	------	-------	-----
8	18	0	0	0	0	0	0	------	---	------	-------	-----
9	5	0	0	100	0	0	0	------	---	------	-------	-----
10	28	0	0	0	36	0	0	------	---	------	-------	-----
11	23	0	0	0	0	0	0	------	---	------	-------	-----
12	21	0	0	0	0	0	0	------	---	------	-------	-----
13	3	0	0	0	30	0	0	------	---	------	-------	-----
14	14	0	0	0	0	0	0	------	---	------	-------	-----
15	4	0	0	100	0	0	0	------	---	------	-------	-----
16	34	0	0	100	16	0	0	------	---	------	-------	-----
17	66	0	0	100	16	0	0	------	EVM	------	-------	-----
18	93	0	0	100	0	0	0 MaxHold	------	EVM	------	-------	-----
19	65	0	0	100	0	0	0 MaxHold	------	EVM	------	-------	-----
20	65	0	0	100	0	0	0 MaxHold	------	EVM	------	-------	-----
21	80	0	0	100	0	0	0 MaxHold	------	EVM	------	-------	-----
22	92	0	0	100	0	0	0 MaxHold	------	EVM	------	-------	-----
23	87	0	0	100	18	0	0 MaxHold	------	EVM	------	-------	-----
24	67	0	0	100	18	0	0 MaxHold	------	EVM	------	-------	-----
25	68	0	0	100	18	0	0 MaxHold	------	EVM	------	-------	-----
26	69	0	0	100	71	0	100 MaxHold	------	EVM	------	-------	Switch
27	66	0	0	100	1	0	100 MaxHold	------	EVM	------	-------	Switch
28	65	0	0	100	0	0	100 MaxHold	------	EVM	------	-------	Switch
29	65	0	0	100	14	0	100 MaxHold	------	EVM	------	-------	Switch
30	81	0	0	100	57	0	100 MaxHold	------	EVM	------	-------	Switch
31	82	0	0	100	0	0	100 MaxHold	------	EVM	------	-------	Switch
32	71	0	0	100	3	0	0 MaxHold	------	EVM	------	-------	-----
33	67	0	0	100	8	0	0 MaxHold	------	EVM	------	-------	-----
34	66	0	0	100	10	0	0 MaxHold	------	EVM	------	-------	-----
35	71	0	0	100	21	0	0 MaxHold	------	EVM	------	-------	-----
36	67	0	0	100	21	0	0 MaxHold	------	EVM	------	-------	-----
37	66	0	0	100	21	0	0 MaxHold	------	EVM	------	-------	-----
38	74	0	0	100	25	0	0 MaxHold	------	EVM	------	-------	-----
39	66	0	0	100	7	0	0 MaxHold	------	EVM	------	-------	-----
40	66	0	0	100	2	0	0 MaxHold	------	EVM	------	-------	-----
41	81	0	0	100	44	0	0 MaxHold	------	EVM	------	-------	-----

Table 2: Trace of the execution of the detection system.

5.8. Demonstration results

5.8.1. Experimental setup

The demonstration phase was performed for a one week long period in Lille-Villeneuve d'Ascq, IFSTTAR laboratory. EHU, TRIALOG and IFSTTAR staff involved in WP3 and WP4 have been participating to this demonstration prepared well in advance by the team. Figure 35 shows the room and the instrumentation that were used for these experiments.

Fig. 35. General view of the experiment.

The room has a surface of approximately 12 x 6 m. All the test equipment was located in the same place. Figure 36 shows the WiFi and WiMAX Access Points (AP) and associated antennas, not visible on the preceding figure 35 (lower right).

Fig. 36. WiFi and WiMAX access points and associated antennas.

WiFi is operating at 2.47 GHz and WiMAX at 5.6 GHz.

Figure 37 shows a view of the table on which were regrouped the different used jammers.

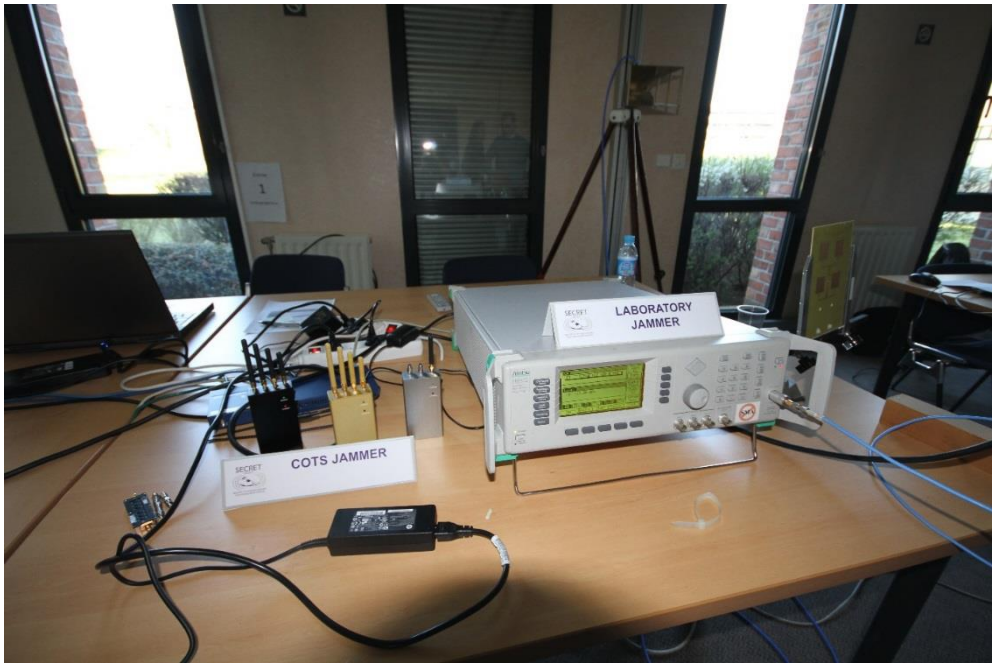


Fig. 37. COTS and laboratory jammers.

We recognize three different portable COTS jammers on the left side and, on the right side, a laboratory equipment which was used to generate predefined wide band jamming waveforms.

Figure 38 shows a view of the p.s.d. sensor.

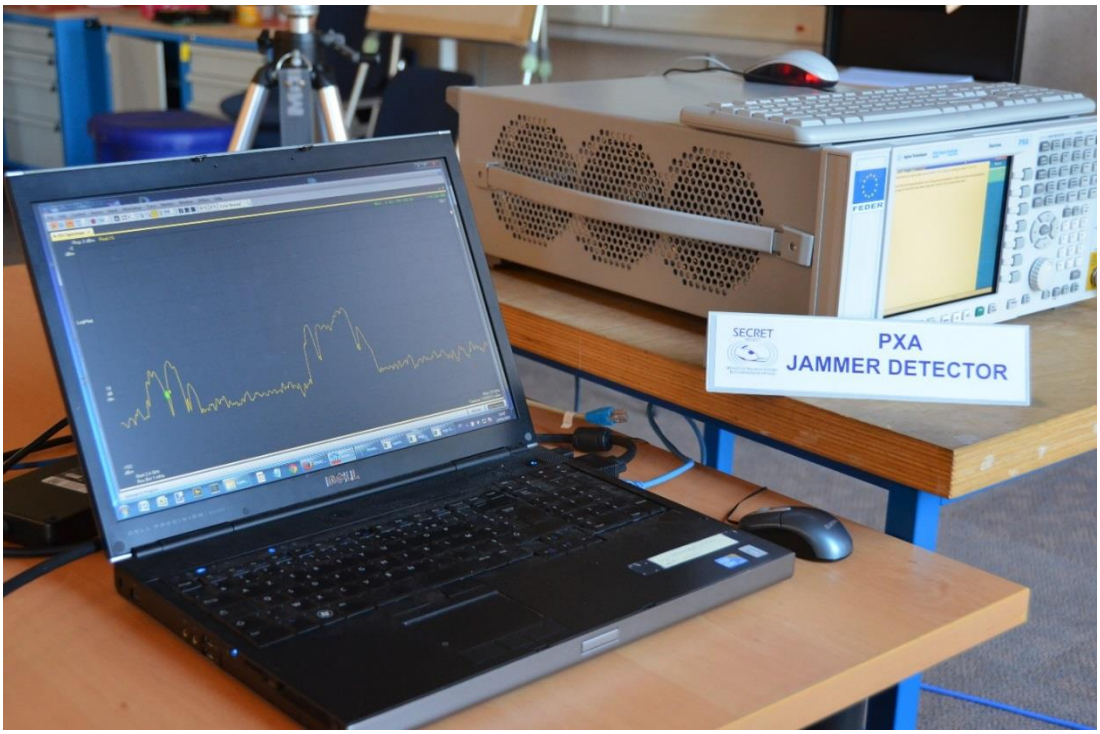


Fig. 38. PSD technique jammer sensor.

The raw data are captured by the PXA situated on the right of the picture. They are loaded in the database. The external computer situated on the left of the picture loads data from the database, performs the considered signal processing and writes the results in the database.

Figure 39 shows a view of the table on which were situated the commercial sensor and the Secret low-cost jammer sensors.

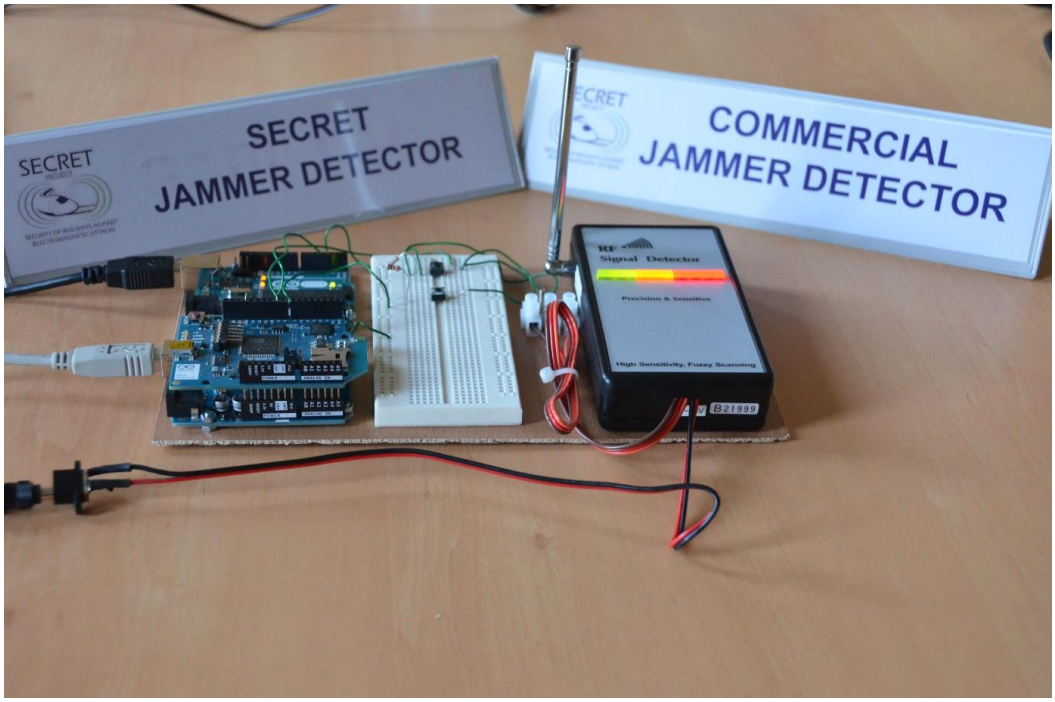


Fig. 39. Secret/Arduino and commercial sensors.

5.8.2. WiMAX and WiFi waveforms to be surveyed

Figure 40 presents a typical received spectrum transmitted from the WiMAX AP and received on the PXA signal analyzer.

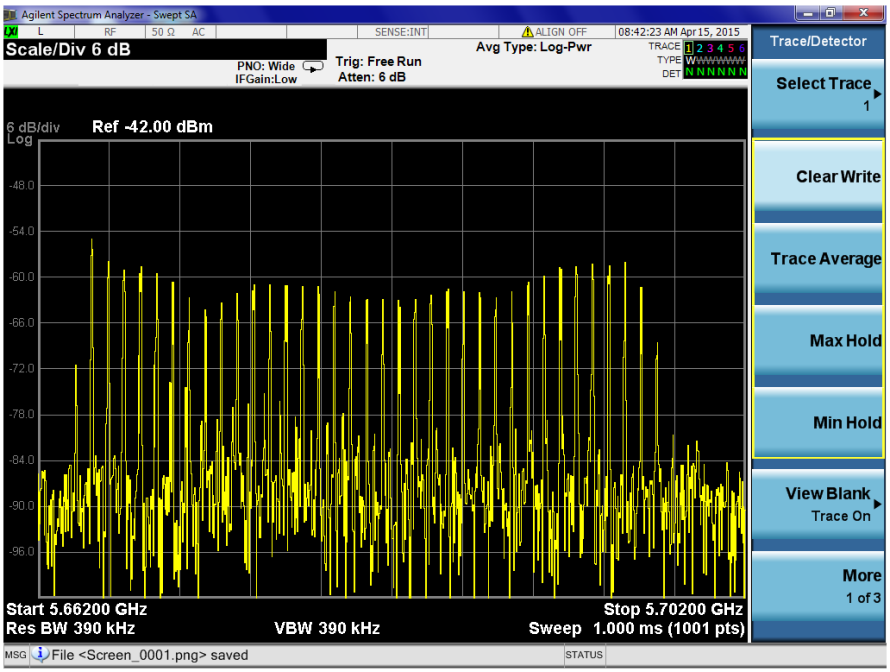


Fig. 40. WiMAX received spectrum on the PXA at 5.6 GHz.

We easily recognize the OFDM modulation with its characteristic comb consecutive carriers. Figure 41

presents the corresponding envelope of this WiMAX signal.

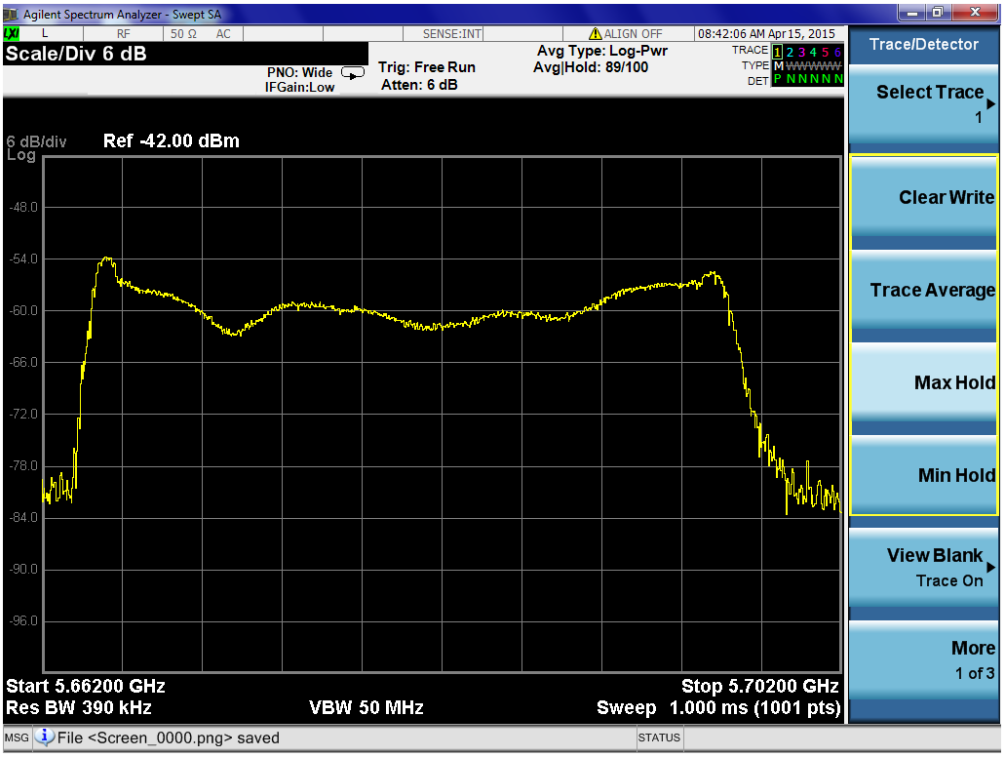


Fig. 41. WiMAX computed template.

Using the maxhold technique, such an envelope will be used as a template to deduce if additional potentially interfering signals do appear in the passband. During our experiments, in the 5.6 GHz band, no other constant local activity was detected. Figure 42 presents the received spectrum transmitted from the WiFi AP operated at 2.47 GHz. Our used channel is located by marker 1.

Fig. 42. WiFi computed template.

As can be deduced from this figure representing the 2.4 to 2.5 GHz swept spectrum, adjacent channels to our used one are also exploited by other APs operating geographically close to the laboratory room.

Figure 43 presents the corresponding received spectrum when a COTS jammer is switched on.

Fig. 43. WiFi band occupancy when a jammer is switched on.

This jammer covers all the WiFi 2.4 to 2.5 GHz band and therefore adds an additional signal covering all the used WiFi frequencies, including our used channel AP.

5.8.3. Results

5.8.3.1. Introduction

This section will now present and analyze some important results extracted from the demonstration campaign. We will successively study the capability of the sensors to detect jamming on the WiFi communication and then on the WiMAX link.

On all the following figures, the outputs of the sensors are synchronized and the recording length is set to 2 minutes. Therefore, it will be possible to evaluate the different time responses of the sensors.

5.8.3.2. WiFi

Figure 44 presents the results obtained before a jammer operated in the WiFi frequency band is switched on.

Fig. 44. WiFi band survey by the six sensors without jamming signal.

Eight different windows can be seen in this figure.

The upper left spectrum window represents the received spectrum as recorded by the spectrum analysis and read from the database every second; the whole 2.4 GHz to 2.5 GHz WiFi band is scanned.

The Max Hold window represents the output of the maxhold detection as detailed at the beginning of this deliverable. Since no jamming signals exist, a limited number of potentially jammed channels are detected, depending on random activity in this frequency band.

The Max Prod window represents the output of this particular sensor; here again, we obtain a low output, well below the selected threshold, corresponding to this ‘normal’ radioelectric environment.

The Error Vector Magnitude (EVM) window delivers repetitive peaks normalized to 100 also corresponding to a non-jammed detected condition.

The commercial sensor output stays to a logic level “0” output.

The Secret/Arduino sensor delivers also a “0” corresponding to a no jammer detected condition.

The spectral space analysis (noted Bayesian) also delivers 0.

No false alarms are detected in these operating conditions. The eighth window represents the current received spectrum acquired almost in real time. All these windows are refreshed every second.

Then, a COTS jammer is switched on inside the demonstration room, delivering a local powerful local jamming signal. The jammer is switched on after approximately 1’ and 20’’, i.e. two third of the 2” time window represented in abscissa of figure 45. This figure presents the results obtained by the sensors.

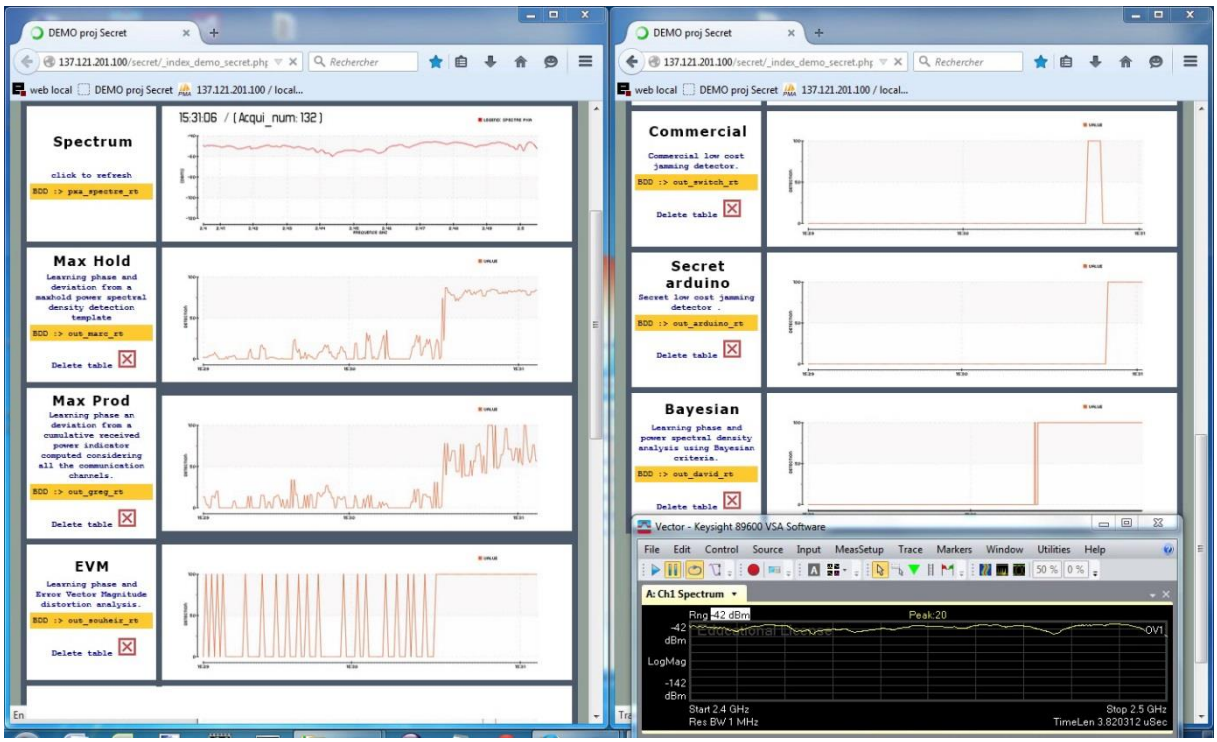


Fig. 45. WiFi band survey by the six sensors in presence of a strong jamming signal.

The spectrum window shows that a wideband powerful signal is now covering the whole 2.4 GHz to 2.5 GHz WiFi band. As a consequence, the WiFi radio link is interrupted.

The Max Hold window indicates that most of the channels are now detected as jammed.

The Max Prod window shows that the global power spectral density as increased a lot in the WiFi scanned band corresponding to this supplementary jamming energy, now exceeding the threshold.

The Error Vector Magnitude (EVM) window delivers a steady “1” signal corresponding to a jammed detected condition.

The commercial sensor output switches to level “1”.

The Secret/Arduino sensor delivers also a level “1” corresponding to a jammed condition. The spectral space analysis (noted Bayesian) also delivers a level “1”.

The eighth window represents the almost real time currently acquired spectrum.

In the presence of the strong jamming signal, all the six sensors are operating efficiently and deliver an alert information to the AS. Using the real time analyzer data and the different corresponding signal processing results in a very quick detection time. The commercial and the Secret/Arduino sensors need more time to deliver an alert information after the jamming signal is applied. The latency time is ranging between 10 to 15 seconds, due to the limited scanning speed capability, i.e. 5 GSM channels per second for example.

Then, the COTS jammer is switched off and we study how the sensors react, coming back to ‘normal’ electromagnetic environment conditions. Figure 46 presents these results. In this figure, the jammer is switched off at approximately 15% from the end of the records.

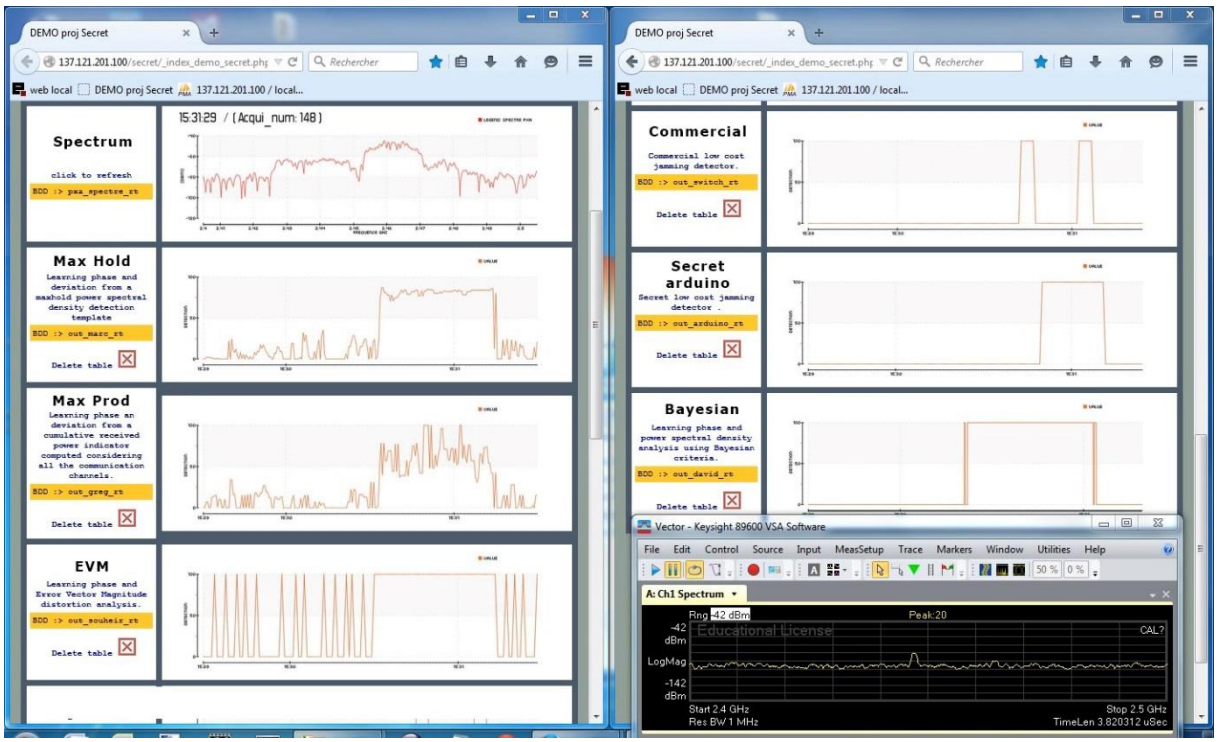


Fig. 46. WiFi band survey by the six sensors after the jammer is switched off.

The spectrum window now shows that a ‘normal’ radio communication activity occupies the whole 2.4 GHz to 2.5 GHz WiFi band and that several channels are busy including the one used by our demonstration video radio link.

The Max Hold window indicates that most of the channels are now detected below the initially computed learning phase template i.e. no jammer activity.

The Max Prod window shows that the global power spectral density has decreased a lot in the WiFi scanned band. This corresponds to a ‘normal’ activity.

The Error Vector Magnitude (EVM) window delivers the periodic peaks corresponding to a non-jammed detected condition.

The commercial sensor output switches back to “0”.

The Secret/Arduino sensor delivers also a level “0” corresponding to a non-jammed condition. The spectral space analysis (noted Bayesian) also quickly comes back to a level “0”.

The eighth window represents the almost real time currently acquired spectrum.

The latency time is short for all the sensors since their outputs rapidly come back to a no jamming detection condition after the jamming signal is suppressed.

Then, the same COTS jammer is switched on again, this time outside from the demonstration room, therefore, reducing a lot the jamming power in the demonstration area. In these conditions, the jammer produce a limited power jamming signal that does not affect significantly the local radio links. We evaluate if the sensors have the capability to detect these particular conditions.

Figure 47 presents the results obtained after this jammer operated in the WiFi frequency band is switched on.

In this figure, the jammer is switched on at approximately 45% from the beginning of the record. The WiFi radio link is fully maintained in these jamming conditions.

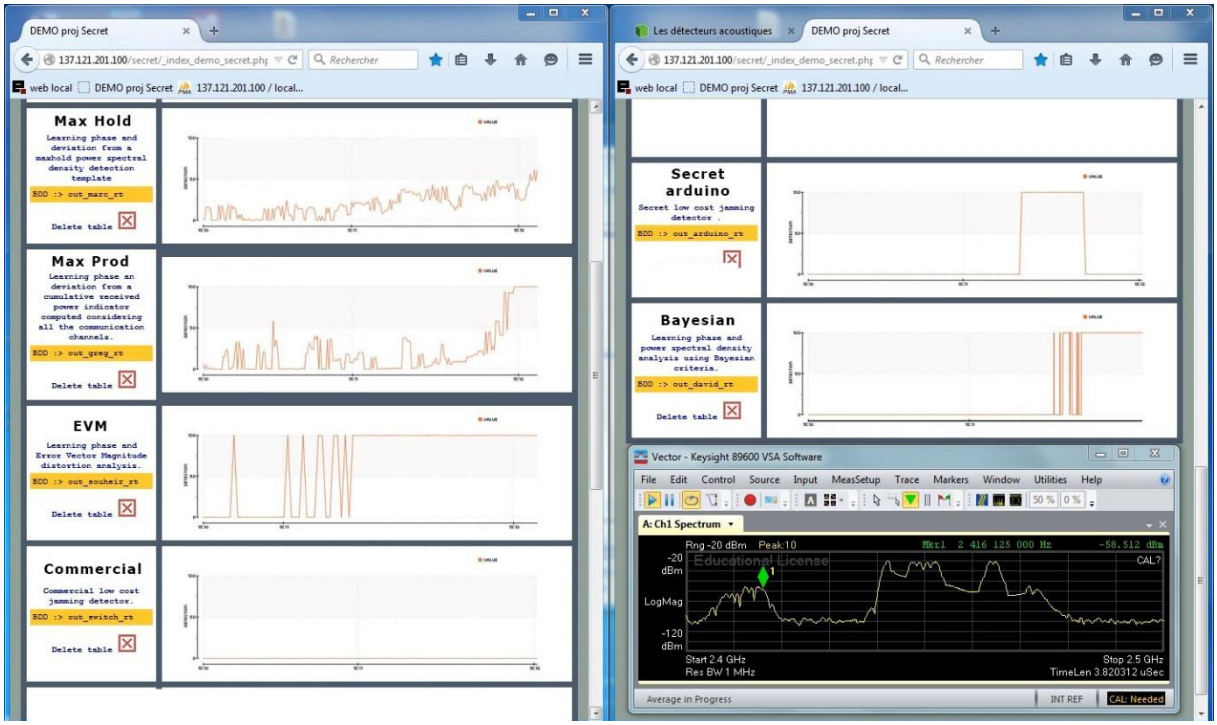


Fig. 47. WiFi band survey by the six sensors in presence of a low power jamming signal.

The previous spectrum window is not represented in this figure.

The Max Hold window indicates that some of the channels are now detected over the initially computed learning phase template. The output of this sensor increases progressively from the time the jammer is switched on. Therefore, the jammed/non jammed limit is not as easy to evaluate as in the previous strong jamming conditions.

The Max Prod window indicates that the corresponding sensor reacts efficiently although with a significant latency time.

The Error Vector Magnitude sensor efficiently detects this low level of jamming signal without latency.

The commercial sensor does not detect the low power jammer.

The Secret/Arduino sensor delivers an output corresponding to a jammed condition with a significant latency time.

The spectral space analysis (noted Bayesian) also detects the jamming signals with a significant latency time in this complex and evolving WiFi electromagnetic environment.

The last spectrum window represents the almost real time currently acquired spectrum barely affected by the wideband jamming signal.

5.8.3.3. WiMAX

Figure 48 presents the results obtain before a jammer operating in the WiMAX frequency band is switched on. We use the same window representation than in the WiFi previous configuration.

We also recall that, to the contrary of the previous WiFi experiments, no nearby constant additional activity could be detected in the WiMAX operated band centered at 5.6 GHz.

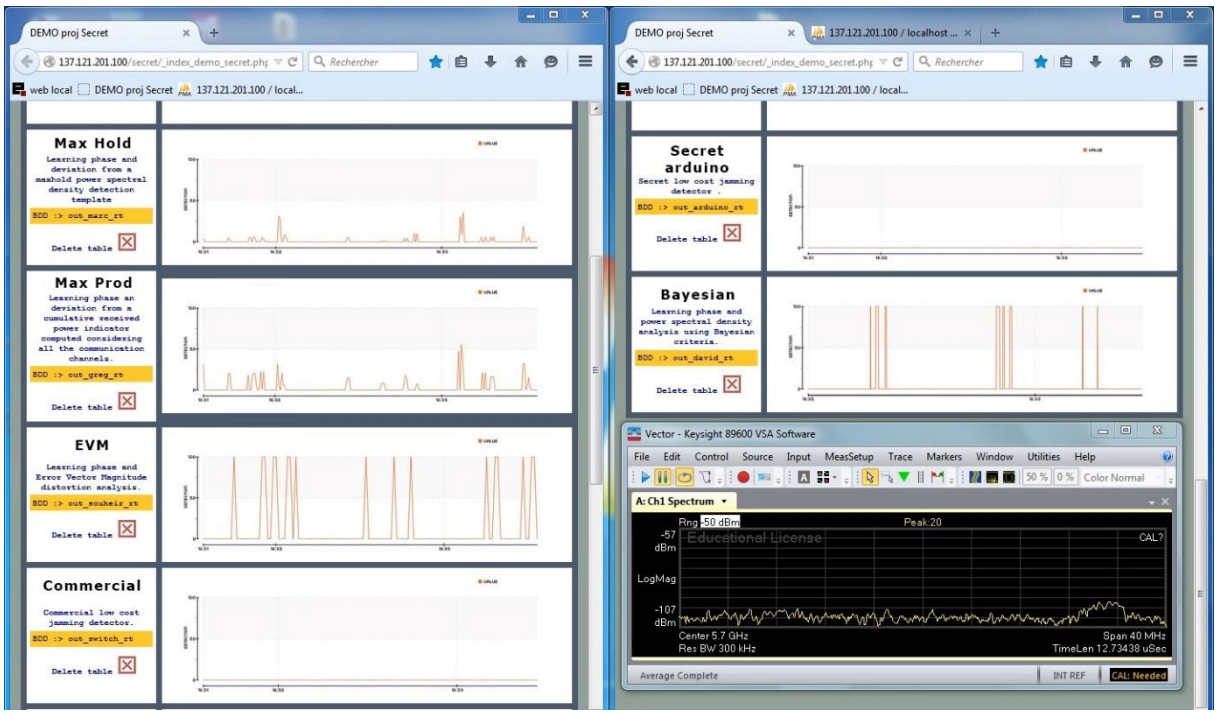


Fig. 48. WiMAX band survey by five sensors without jamming signal.

The Max Hold window represents the output of the maxhold detection; since no jamming signals exists, a limited number of potentially jammed channels is detected depending on random activity in this frequency band.

The Max Prod window delivers a low output corresponding to this non jamming condition.

The Error Vector Magnitude (EVM) window delivers repetitive peaks normalized to 100 corresponding to a non-jammed detected condition.

The commercial sensor output stays to 0.

The Secret/Arduino sensor is not operational in this frequency band and should not be considered.

The spectral space analysis (noted Bayesian) also delivers 0 with random peaks probably due to the complexity of the OFDM spectrum presented in the past figure 41.

The last window represents the current received spectrum acquired almost in real time (the first spectrum top left window is refreshed every one second from the database).

Then, a COTS demonstration room located jammer is switched on. Figure 49 presents the results obtained after this jammer operated in the WiMAX frequency band is switched on at approximately 50% from the beginning of the record. We recall that the recording length is 2 minutes for all these presented results.

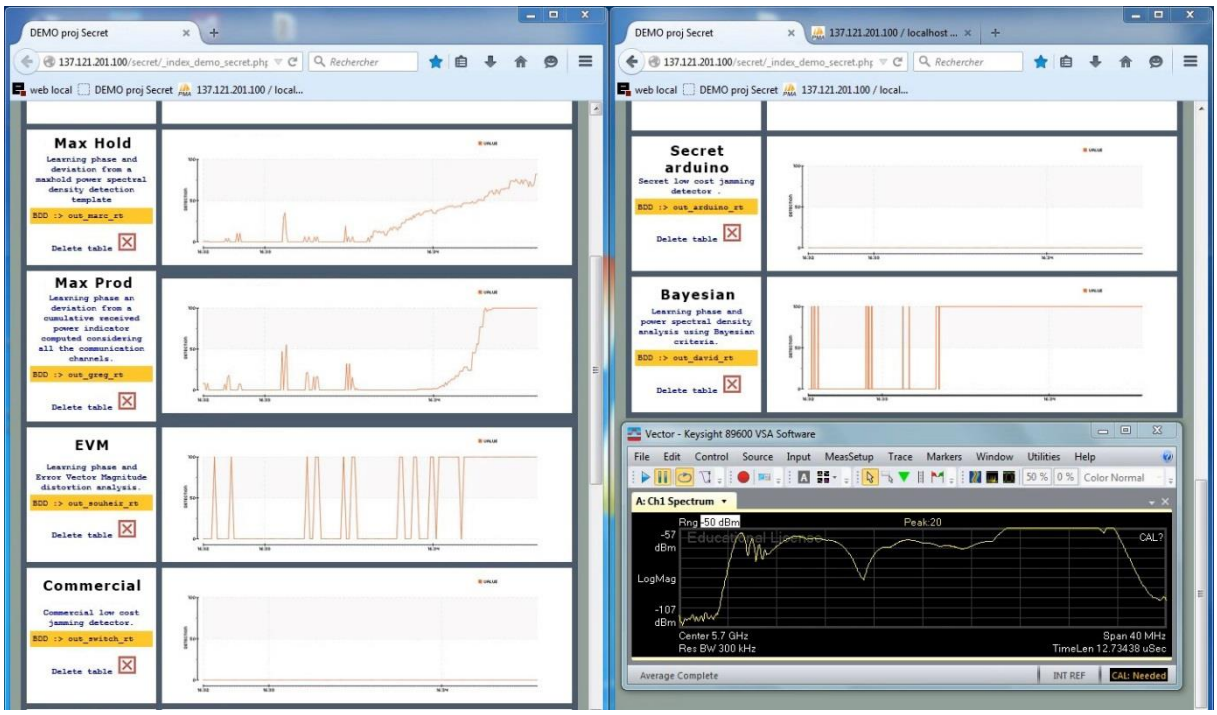


Fig. 49. WiMAX band survey by five sensors in presence of a jamming signal.

The Max Hold window shows that progressively, a large number of potentially jammed channels is measured, starting when the jamming signal is applied.

The Max Prod window delivers a high output corresponding to a jamming detection condition after some latency.

After a latency time also, the Error Vector Magnitude (EVM) window delivers a steady value, normalized to 100, corresponding to a jammed detected condition.

The commercial sensor output stays a long time to level “0”; it switches to level “1” after 32 seconds.

The Secret/Arduino sensor is not operational in this frequency band and must not be considered.

The spectral space analysis (noted Bayesian) quickly delivers a steady level “1” corresponding to a jammed detected condition. This sensor is operating in favorable conditions since there is only one WiMAX signal present in the considered bandwidth.

The last window represents the current received spectrum acquired almost in real time (the first spectrum top left window is refreshed every one second from the database).

Then, as for the WiFi experiment, the laboratory jammer is switched off and we study how the sensors detect this coming back to “normal” conditions.

Figure 50 presents the results obtained after this jammer operated in the WiMAX frequency band is switched on at approximately 15% from the end of the record.

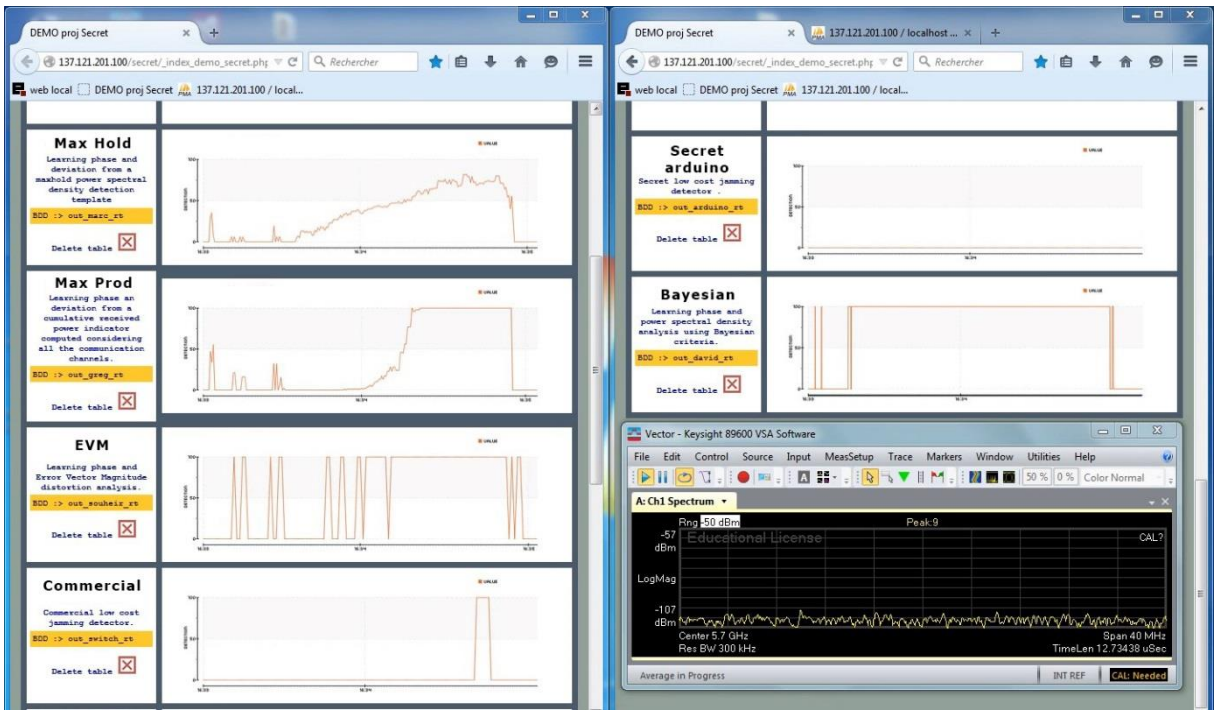


Fig. 50. WiMAX band survey by five sensors after the jamming signal is switched off.

The Max Hold window indicates that most of the channels are now detected below the initially computed learning phase template, i.e. no jamming condition.

The Max Prod window shows that the global power spectral density has decreased a lot in the WiMAX scanned band and that it now corresponds to a ‘normal’ activity.

The Error Vector Magnitude (EVM) window delivers the periodic peaks corresponding to a non-jammed detected condition.

The commercial sensor has very lately detected a jamming condition; its output has now come back to “0”.

The Secret/Arduino is not operational at 5.6 GHz (GSM and WiFi 2.4 to 2.5 GHz bands only).

The spectral space analysis (noted Bayesian) also comes back to “0”.

The seventh window represents the almost real time currently acquired spectrum showing no electromagnetic activity at this particular acquisition time.

The latency time is short for all the sensors since their outputs rapidly come back to a no jamming detection condition after the jamming signal is suppressed. The commercial sensor has a low response time.

5.8.4. Conclusion

Table 3 concludes this analysis and synthesizes the obtained results.

	Reference commercial sensor	Max Hold technique	Max Prod technique	EVM technique	Spectrum space technique
Detection capacity	Good detection in presence of a strong jammer	Good. Sensitivity depends on the number of non-occupied channels in the scanned bandwidth	Good. Sensitivity depends on the number of non-occupied channels in the scanned bandwidth	Excellent detects even in presence of low power jammers	Excellent if the electromagnetic environment is stable (no mobility)
Latency time	Significant delay (10" and more)	Delay depends on the number of channels to scan	Delay depends on the number of channels to scan	Excellent with a real time acquisition system	Excellent with a real time acquisition system
Advantages	Wide band (several GHz)	Good performance	Good performance	High performance	High performance
Drawbacks	A strong out of band signal can easily be considered as a jamming signal	Scan the band channel per channel	Scan the band channel per channel	Cost Must be adapted to the radio communication protocol in use	Cost Necessitate a good learning phase

Table 3: Qualitative comparison of the different tested sensors.

We obtain that depending on the considered sensor hardware and software, effective detection of jamming conditions can be detected locally and delivered to the AS. Receiving information from different sensors, the AS/DS engine then decide whether or not this information needs consideration.

We also obtain that using different sensor techniques, we can provide an early warning that can be further completed by other sensors data that limit the false detection probability.

6. NetBox demonstration

6.1. Introduction

The second Secret WP3 sensor demonstration was selected in order to extend the scope of our initial demonstration. Its main differentiators are the following ones. It is using on the one hand, a railway radio communication representative equipment i.e. an ALSTOM NetBox and, on the other hand, a non-proprietary radio link, i.e. a 3G radio communication instead of the previous local WiMAX radio link.

6.2. NetBox and used 3G signals presentations

6.2.1. The NetBox

The NetBox, designed for railway applications, provides wireless communication interfaces for all products embedded inside a rolling stock. It is used for the design, the installation and maintenance of all on-board and ground equipment. The following figure 51 shows a NetBox railway typical usage and, figure 52, a view of this equipment. The hardware is installed in a 3U standard rack.

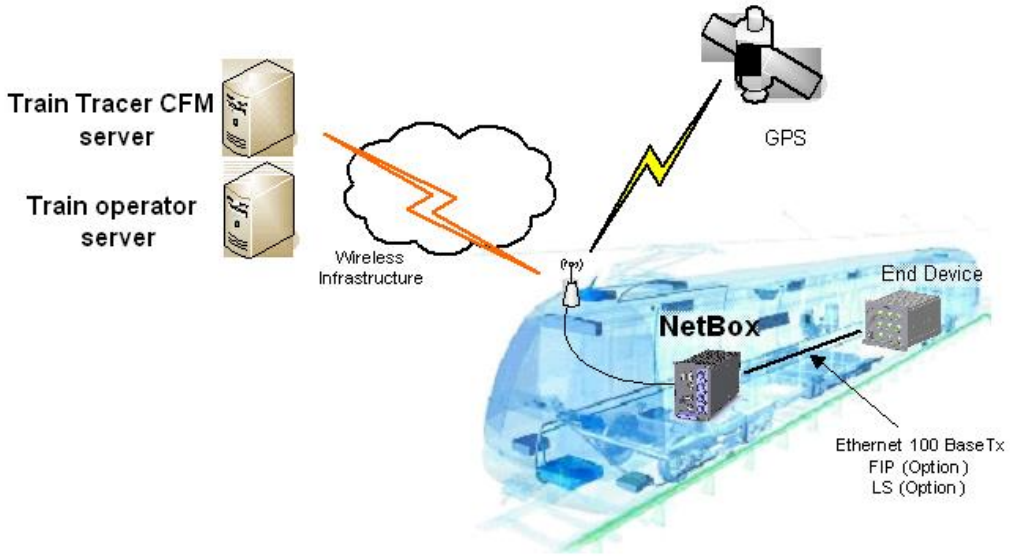


Fig. 51. NetBox typical usage.

Fig. 52. Picture of NetBox base.

The NetBox base includes:

- A power supply 24-110VDC / 45W
- A CPU300 CPU board equipped with INTEL ATOM processor
- A Mini PCI Wi-Fi Board
- A Mini PCIe GSM 3G board
- Two SIM card slots
- A GPS receiver
- Two Ethernet interfaces
- A serial RS485/422/232 interface
- An I²C (“dataplug”) and serial RS232 interface
- A digital I/O

For our experiments, the NetBox was also integrating a secondary Mini PCIe GSM 3G. Alternatively, it can be fitted with a GSM-R board. Therefore, this equipment is able to communicate using WiFi and 3G. For example, the WiFi link is used to transfer the rolling stock maintenance data when trains are arriving in stations and the 3G link is used when trains are outside a WiFi communication link or at speed higher than 30 km/h.

6.2.2. The 3 G network

The used 3 G network is operated at 2.1 GHz. Figure 53 indicates the local channels in activity as well as the received power level.

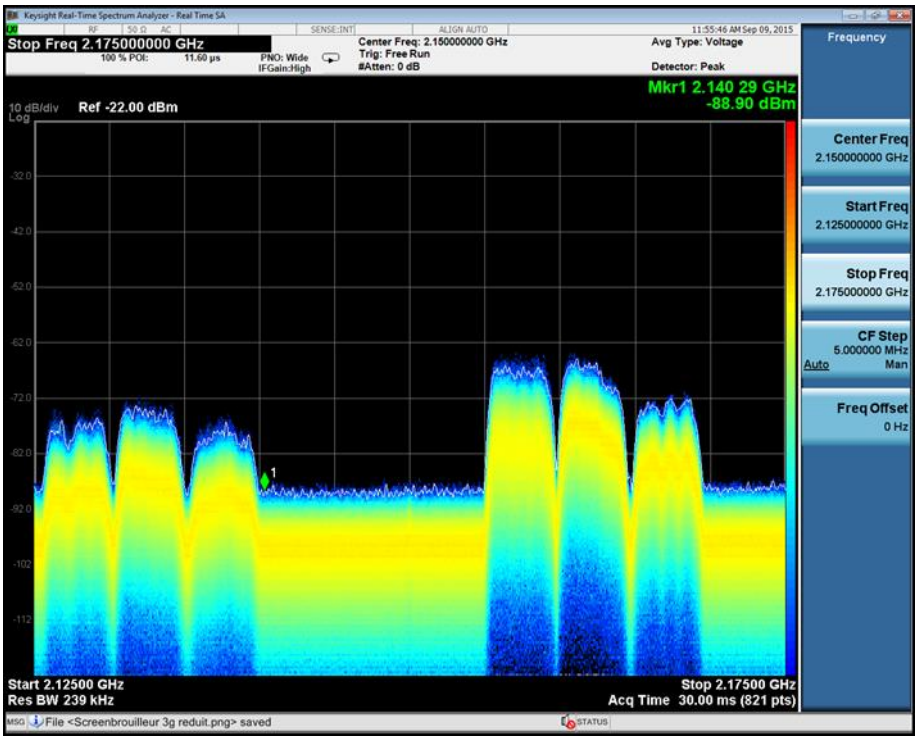


Fig. 53. 3G non jammed received spectrum at the demonstration location.

6.3. Demonstration conditions

This second demonstration phase was performed in Alstom-Charleroi premises in September 2015. Figure 54 to 56 show views of the laboratory installation with the Secret installation.

Figure 54 presents the area where the NetBox is installed. This equipment is associated to a power supply and a router. It is equipped with 3G and WiFi antennas.

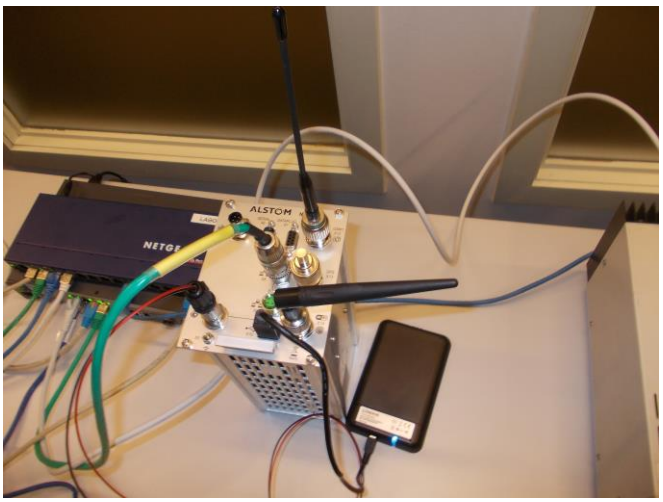


Fig. 54. NetBox laboratory area.

Figure 55 shows, in the rear, the jamming area equipped with laboratory and cots jammers. The real time spectrum surveillance equipment can also be seen on the right.

Fig. 55. Jamming and radiofrequency surveillance area.

Figure 56 shows the sensor area. In the middle stands the computer dedicated to the database operation.

Fig. 56. Sensors area.

The same sensors and database as for the first demonstration were used. However, instead of running the MySQL database on the IFSTTAR laboratory computation cluster, it runs on a local dedicated PC seen in figure 56. This has for consequence to slow down the refreshing period of the whole system which was in the order of two seconds instead of one second during the first demonstration.

In the NetBox existing hardware equipment scenario, it is difficult to implement the same multipath communication system as it was done for the initial demonstration. Instead of that, SeaMo was implemented on a Linux based laptop with WLAN and 3G on the NetBox. SeaMo is a vertical handoff implementation for heterogeneous wireless networks [16]. The testbed also comprises network elements that support HIP based mobility management for IPv4 as used by the 3G provider. Deliverable D4.5 presents a detailed analysis of this specific NetBox setup.

Moreover, the tests were performed using the Secret WP3 detectors associated to a local simplified AS/DS system. The AS/DS delivers an information to the NetBox stating that jamming conditions have appeared in the 3G or, alternatively, in the WiFi band and that a handoff to the backup radio link is needed. This has for consequence to switch the NetBox radio configuration from an initial radio link to the backup link i.e. 3G to WiFi or WiFi to 3G.

6.4. Measurements description

6.4.1. Primary communication using 3G

For this demonstration, instead of focusing on the pure sensor performance as in the first demonstration, we concentrated on time measurements and on the role of the sensors in this architecture. Time measurements were selected to evaluate the durations of potential losses of communication. Figure 57 represents the time diagram using 3G as a primary communication and WiFi as the backup communication means.

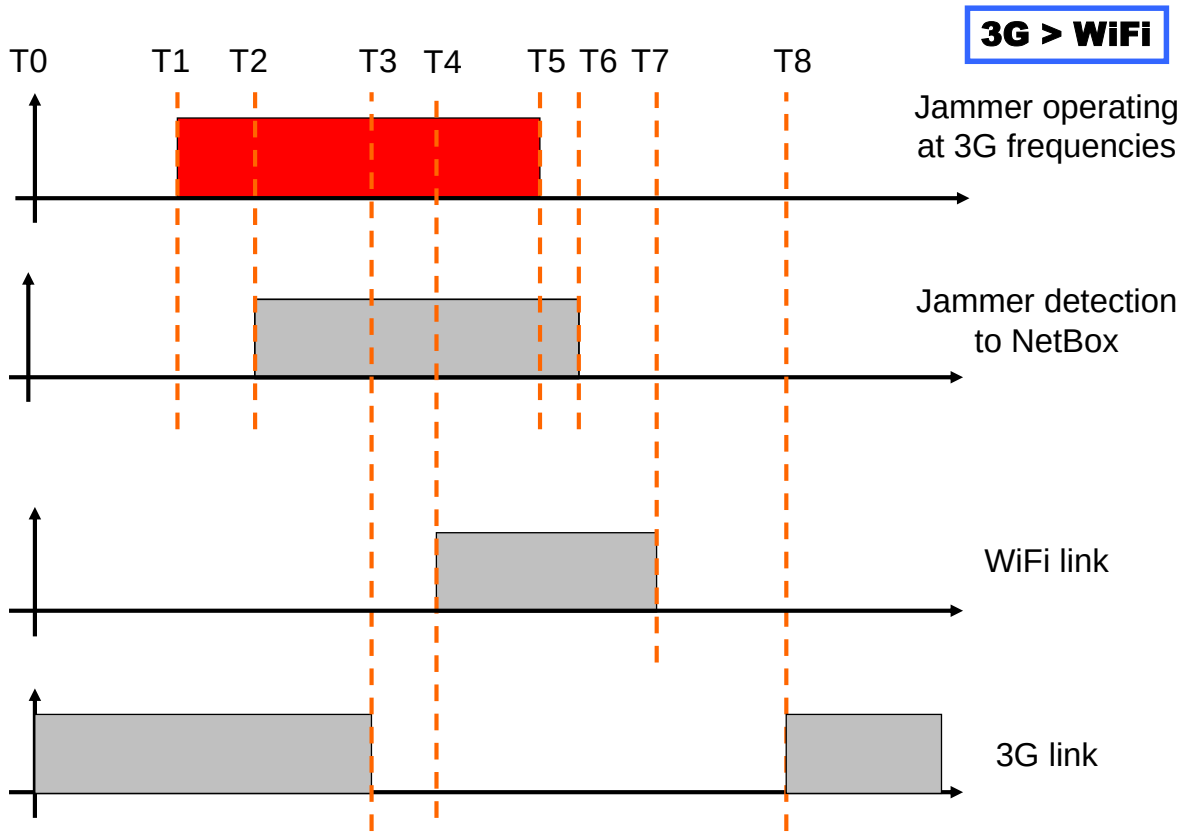


Fig. 57. 3G to WiFi and back measurement timing.

The selected reference times are the following: the equipment is switched on at T0 and the communication is initiated in 3G. At T1, a jammer operating in the 3G band is switched on. At T2, at least one Secret sensor detects the jamming situation. Between T2 and T3, this information is

delivered to the AS/DS and then to the NetBox; as a consequence, the decision is taken to switch from 3G to WiFi. At T3, the 3G link is interrupted. At T4, the WiFi link is started. Between T3 and T4 we are no more in 3G and not yet in WiFi, we lose the communication. This corresponds to the association time requested to access the WiFi network. At T5, the 3G jammer is switched off. At T6, all the Secret sensors indicate that there is no more jamming affecting the 3G band. At T7, the AS/DS/NetBox configuration stops operation using WiFi and to switch back to 3G. At T8, the NetBox resumes in 3G, data transfer is now operating through this link. Between T8 and T7, we are losing the communication. This corresponds to the re-association time requested to access the 3G network

6.4.2. Primary communication using WiFi

The reverse configuration, i.e. operating primarily the WiFi link and using 3G as a backup radio link is presented in figure 58.

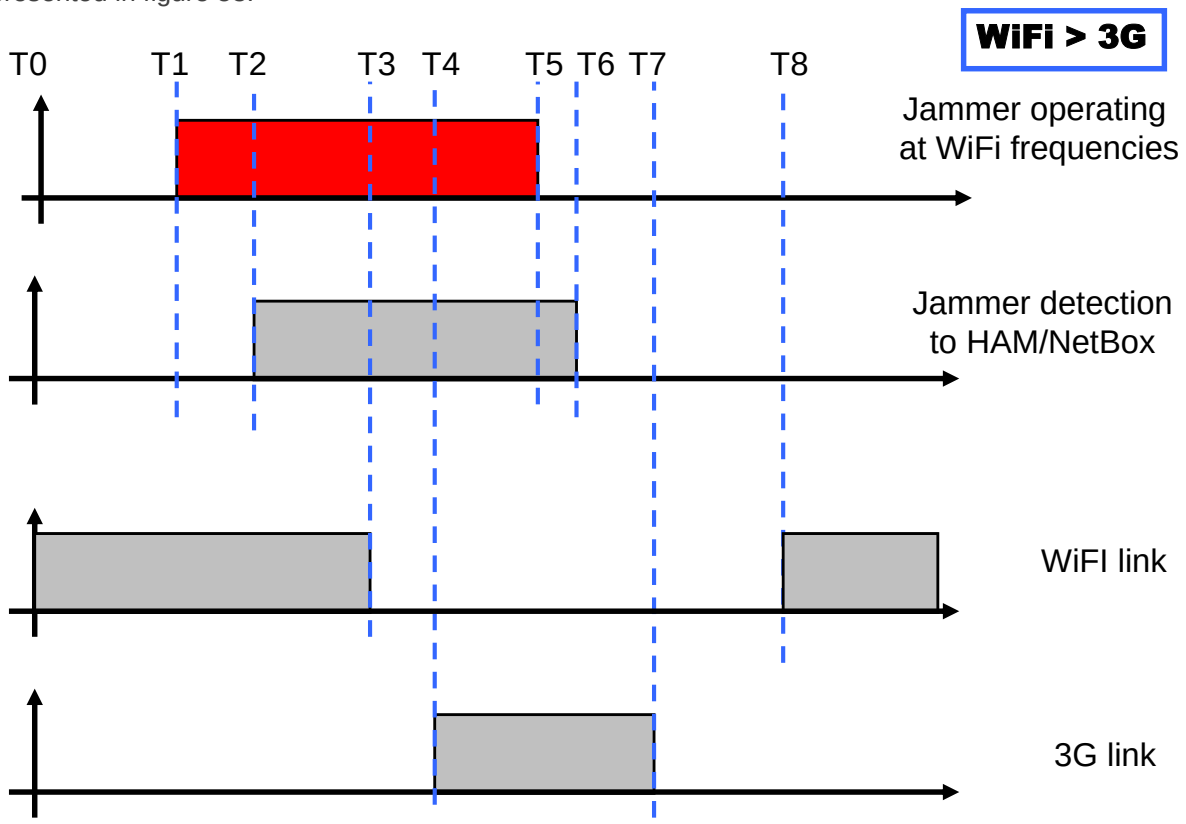


Fig. 58. WiFi to 3G timing of the measurements.

This time, the equipment is switched on at T0 and the communication is initiated using the WiFi network. At T1, a jammer operating in the WiFi band is switched on. At T2, at least one Secret sensor detects the jamming situation. Between T2 and T3, this information is delivered to the local AS; as a consequence, the decision is taken by the DS and sent to the NetBox to switch from 3G to WiFi. Therefore, at T3, the WiFi link is interrupted. At T4, the 3G link becomes operational. Between T3 and T4 we are no more in WiFi and not yet in 3G, we lose the communication. This corresponds to the association time to the 3G network. At T5, the WiFi jammer is switched off. At T6, all the Secret sensors indicate that there is no more jamming affecting the WiFi band. At T7, the AS/DS/NetBox configuration decides to stop operation in 3G and to switch back to the WiFi network. At T8, the NetBox resumes in WiFi, data transfer is now operating through this link. Between T8 and T7, we are losing the communication. This corresponds to the re-association time to access the WiFi network.

6.5. Jamming the NetBox primary 3G radio link

6.5.1. First configuration – Preserving the 3G used channels

In a first experiment, the setup is configured to use 3G as the primary radio link and WiFi as the secondary backup link. In the laboratory area, we locally jam 3G downlink channels that are not used for the communication. This jamming scenario can be seen in figure 59 and compared to the one

presented in figure 53, obtained in absence of jamming. This way, Secret 3G jamming sensors can sense the jamming in the band, deliver this information to the local AS and indicate to the NetBox that it must switch to WiFi operation to continue operation in a non 3G jammed environment. However, since the 3G used radio communication channels are not jammed, this transition is operated without interfering with our established communication thus, facilitating the vertical handoff (VHO) operation and potentially limiting the loss of communication duration.

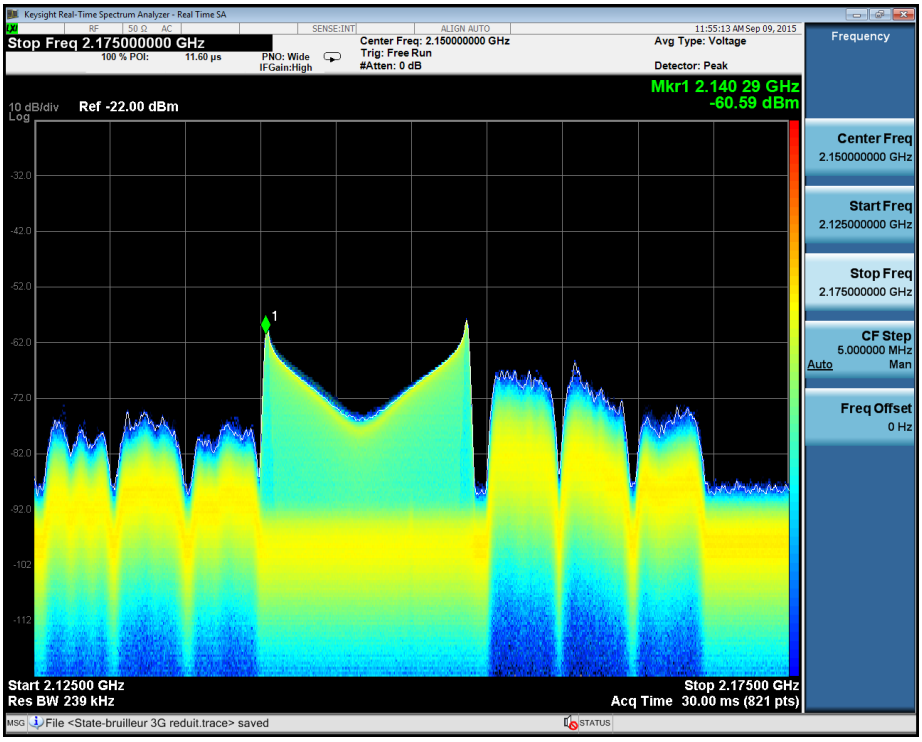


Fig. 59. 3G partially jammed spectrum – Not affecting the used 3G radio link.

We obtained the following results presented in table 4:

T1 to T2	T2 to T3	T3 to T4	T4 to T5	T5 to T6	T6 to T7	T7 to T8
2''	2.3''	4.2''	30'' to 1'	2''	43''	4.6''
3''	1.1''	4''	30'' to 1'	2''	9.5''	4.4''
3''	2.1''	3.7''	30'' to 1'	2''	26''	4.4''
2''	1.8''	3.7''	30'' to 1'	2''	48.5''	4.7''
2''	1.1''	4''	30'' to 1'	2''	9''	5''

Table 4: Timing measurements obtained when jamming 3G non used channels.

In this table 4, the two first lines correspond to results of tests performed using only pings sent every 100 ms. The three last lines correspond to results of tests performed with an additional video flux sent at 250 kbps.

We deduce from this table 4 the following results:

- As explained earlier, T1 to T2 and T5 to T6 (2" to 3") are determined by the local database processing time and are not representative of the real response time of the sensors. They were studied in more detail during the first demonstration.
- At T2, the jamming information sent by the sensors is received by the AS. T2 to T3 is the 3G to WiFi response time of the DS/NetBox implemented configuration. It ranges between 1.1" and 2.3''.
- T3 to T4 ranges from 3.7'' to 4.2''. It corresponds to the loss of communication duration while switching from 3G to the local WiFi network. Since the 3G band is partially jammed but not our used communication channel then, 3G maintains the data transfer as long as possible. Therefore, T3 to T4 is representative of the connection time to the WiFi network. We have to mention that our WiFi used channel was exploited also by other close APs in the ALSTOM premises.
- T4 to T5 is selected by the user. We maintain the jammer on between 30'' and 1' after the radio link has toggled.
- T6 to T7 is ranging from 9'' to 48.5''. This is the time requested to reconnect to the commercial 3G access provider. By working at different periods of the day, we have suspected that during peak traffic activity, at noon for example, the connection time increases significantly. This could also be the case in some conditions on board a train and lead to high connection time.
- T7 to T8 is ranging between 4.4'' and 5'', this is close to the T3 to T4 range. In this case also, while 3G is not yet available, WiFi, not jammed, maintains the communication. Therefore, the overall loss of communication duration is limited.
- There is no significant impact when the video flux exchange is operated or not.

6.5.2. Second configuration – Jamming all the 3G used channels

In this second configuration, the jamming signal is applied from T1 to T5 over all the 3G frequency channels. Therefore, our 3G link is perturbed and the connection is lost almost immediately after the jammer is switched on. Since the 3G protocol implements frequency hopping, it was necessary to jam all the channels simultaneously. Otherwise, the protocol will search for non-jammed 3G channels and maintain the radio communication over this non-jammed channels. Figure 60 represents the jamming signal spread out over the whole 2.1 GHz band.

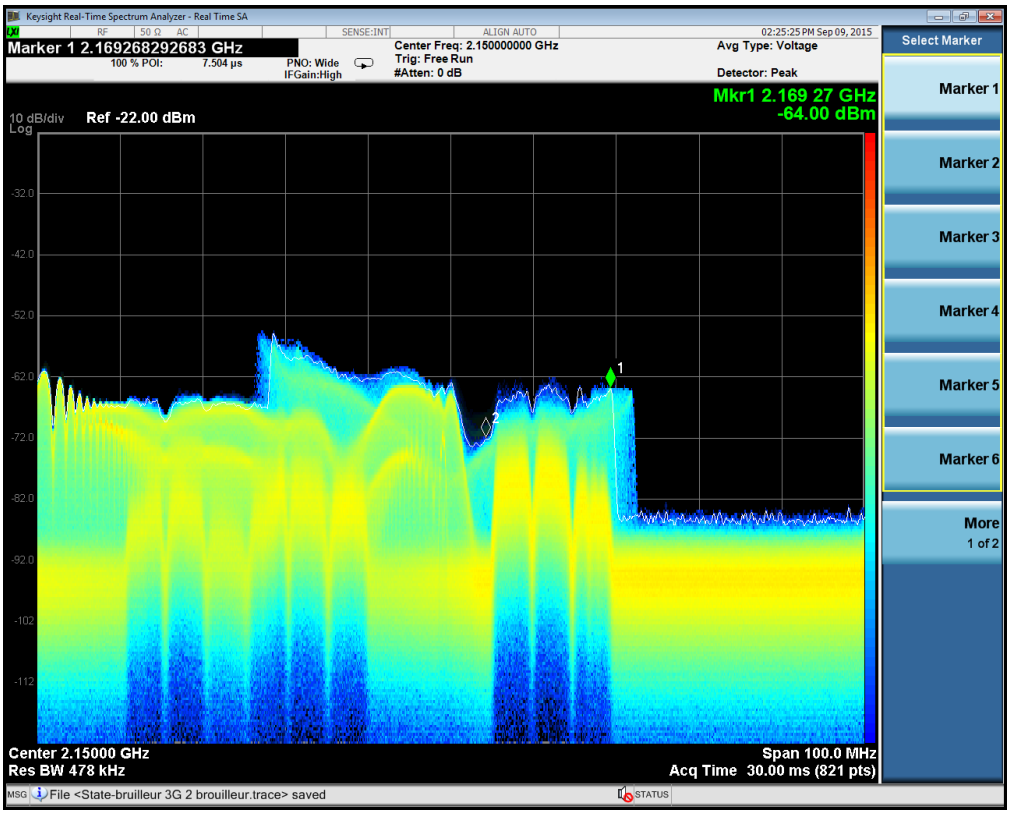


Fig. 60. 3G fully jammed spectrum – Interrupting locally any 3G communication.

Table 5 presents the corresponding timing results.

T1 à T2	T2 à T3	T3 à T4	T4 à T5	T5 à T6	T6 à T7	T7 à T8
2''	1.2''	3.7''	30'' to 1'	3''	30.8''	4.6''
2''	1.2''	5.2''	30'' to 1'	3''	2.7''	6.1''
2''	1.3''	7.5''	30'' to 1'	2''	1.4''	Software failure
2''	2.3''	10''	30'' to 1'	3''	8.7''	4.7''

Table 5: Timing measurements obtained when jamming all the 3G channels.

In this table 5, the two first lines correspond to results of tests performed using only pings sent every 100 ms. The two last lines correspond to results of tests performed with an additional video flux sent at 250 kbps.

We deduce from this table 5 the following results:

- T1 to T2 and T5 to T6 as before. In this scenario, the information provided by the sensors will be delivered after two seconds but the 3G communication is already lost since T1, when the jammer is switched on.
- T2 to T3 ranges between 1.2" and 2.3'', this is the response time of the AS/DS/NetBox implemented configuration already measured and reported in Table 4.
- T3 to T4 ranges from 3.7'' to 10'' instead of 3.7'' to 4.2'' in table 4. This is the loss of communication duration while switching from 3 G to the local WiFi. Since the sensor does not inform the AS in due time, the loss of communication duration can be significantly increased. This time, the 3G radio link cannot maintain the communication while accessing to the WiFi network.
- T4 to T5 is selected by the user. We maintain the jammer on between 30'' and 1' after the radio link has toggled.
- T6 to T7 is ranging from 1'' to 30.8''. This is the time to reconnect to the commercial 3G provider. As indicated in the previous experiment, it probably depends heavily on the 3G local network load.
- T7 to T8 is ranging between 4.6'' and 6.1''. Indeed, WiFi, not jammed, is maintaining the communication as long as 3G is not reconnected. Therefore, the overall loss of communication duration is limited.
- There is no significant impact when the video flux exchange is operated or not.

Considering results presented in both table 4 and table 5, we conclude on the interest to develop almost real time detectors to facilitate the vertical handoff (VHO) when jamming occurs on the primary radio link.

6.6. Jamming the NetBox primary WiFi radio link

We now consider the reverse condition. WiFi is the primary link, 3G is the backup radio link.

6.6.1. First configuration – Preserving the WiFi used channel

As for the previous scenario, in a first step, we jam most of the WiFi channels but not our selected WiFi communication channel. Therefore, Secret WiFi jamming sensors can sense the jamming, deliver

this information to the local AS and the DS indicates to the NetBox that it must switch to 3G operation to further operate in a non WiFi jammed environment. This way, as the WiFi used radio communication channel is not jammed then, the transition from WiFi to 3G is operated without altering the communication effectiveness and the VHO is facilitated.

We obtained the results presented in table 6.

T1 to T2	T2 to T3	T3 to T4	T4 to T5	T5 to T6	T6 to T7	T7 to T8
2''	3.7''	5''	30'' to 1'	4''	2.5''	4.1''
2''	3.9''	5''	30'' to 1'	2'	2.5''	3.7''
4''	9''	4.8''	30'' to 1'	4''	1.5''	3.7''
3''	9''	4.2''	30'' to 1'	2''	2''	3.4''
2''	9.2''	4.7''	30'' to 1'	2''	1.7''	4''

Table 6: Timing measurements obtained when jamming WiFi non used channels.

In this table 6, the two first lines correspond to tests performed using only pings sent every 100 ms. The three last lines correspond to tests performed with an additional video flux sent at 250 kbps.

We deduce from this table 6 the following results:

- T1 to T2 and T5 to T6: the same comments as in table 4 apply.
- T2 to T3 ranges between 3.7" to 9.2'', this is the response time of the AS/DS/NetBox implemented configuration. The repetitively increased and high measured duration obtained in the three last test was not fully explained. The existence of the video flux cannot explain the difference in performance (see below).
- T3 to T4 ranges from 4.7'' to 5''. These values are remarkably stable. These results were obtained during morning experiments supposed to correspond to low 3G users activity. This is the loss of communication duration while switching from WiFi to 3G. These values correspond to low connection times to the 3G network.
- T4 to T5 is selected by the user. We maintained the jammer on between 30'' and 1' after the radio link has toggled.
- T6 to T7 is ranging from 1.5'' to 2.5''. This is the short duration necessary to reconnect to the WiFi local network.
- T7 to T8 is ranging between 3.4'' and 4.1''. Indeed, 3G is maintaining the communication as long as WiFi is not ready. Therefore, the loss of communication duration is limited.

6.6.2. Second configuration – Jamming all the WiFi channels

In this second configuration, the jamming signal is applied from T1 to T5 over the whole 2.4 to 2.5 GHz WiFi band. Figure 62 represents the jamming signal spread out over the whole WiFi band. The WiFi communication is almost immediately interrupted. Since the used WiFi protocol does not implement frequency hopping, it could have been sufficient to jam the identified used frequency channel.

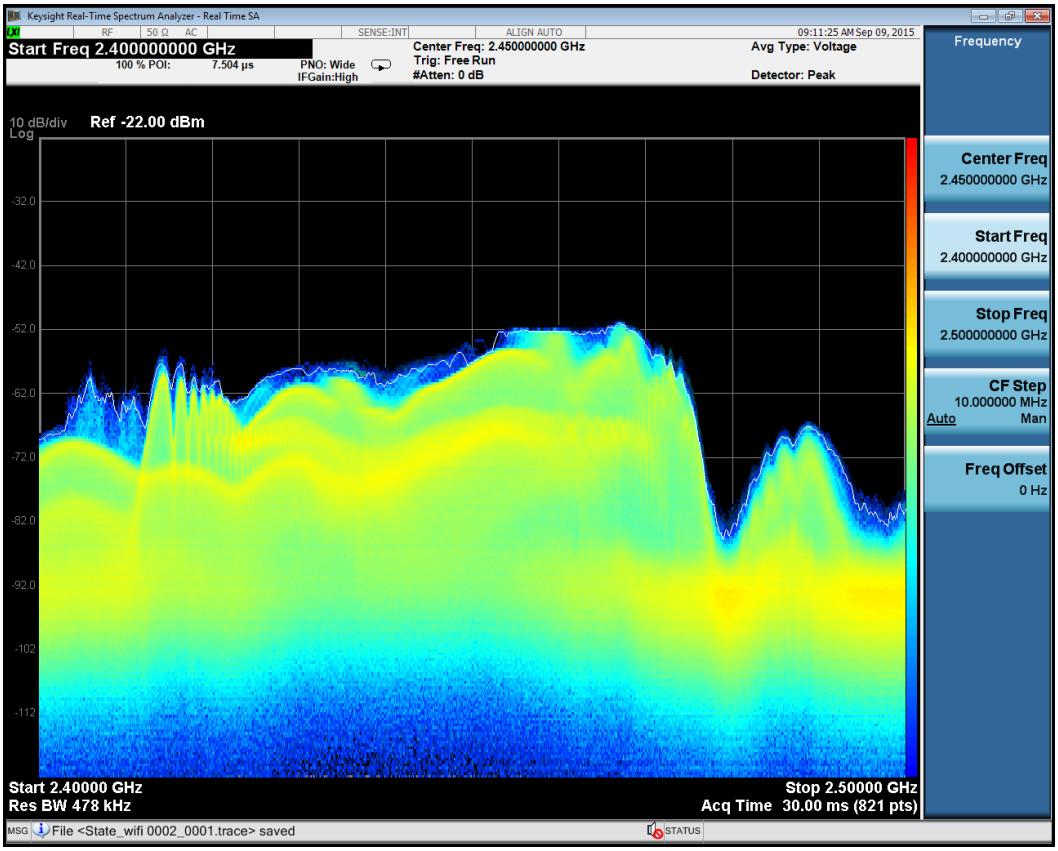


Fig. 61. WiFi fully jammed spectrum – Interrupting the WiFi link.

We obtained the results presented in table 7.

As in table 6, the two first lines correspond to tests performed using only pings sent every 100 ms. The three last lines correspond to tests performed with an additional video flux sent at 250 kbps.

T1 to T2	T2 to T3	T3 to T4	T4 to T5	T5 to T6	T6 to T7	T7 to T8
3	4.1	17.1	30'' to 1'	2	1	4.4
3	8.1	19.9	30'' to 1'	2	9.8	3.7
2	3.7	12	30'' to 1'	3	1	3.6
3	3.8	16.4	30'' to 1'	2	11.2	3.8
3	4	14.2	30'' to 1'	2	1.6	4

Table 7: Timing measurements obtained when jamming all the WiFi channels.

We deduce from this table 7 the following results:

- T1 to T2 and T5 to T6, as explained before, are limited by our experimental setup.
- T2 to T3 ranges between 3.7" to 8.1'', this is the response time of the AS/DS/NetBox implemented configuration. As in table 6, in this configuration, we also obtain a high 8.1" atypical value that is not fully explained.
- T3 to T4 ranges from 12'' to 19.9''. Connecting to the 3G link can be long and the jammed WiFi link is no more active. Therefore, the loss of communication duration is high.
- T4 to T5 is selected by the user. We maintain the jammer on between 30'' and 1' after the radio link has toggled.
- T6 to T7 is ranging from 1'' to 11.2''. This is the time to reconnect to the WiFi local network. As several APs were detected in the surroundings and could be also locally jammed, reconnecting to the WiFi network can necessitate a more or less significant delay.
- T7 to T8 is ranging between 3.6'' and 4.4''. Indeed, 3G is maintaining the communication as long as WiFi is not ready. Therefore, the loss of communication duration is limited.

6.7. Conclusion

Considering results presented in tables 4 and 5 and in tables 6 and 7, we conclude on the high interest to install almost real time detectors to facilitate the vertical handoff when jamming occurs on the primary link.

Otherwise, significant loss of communication durations, measured up to 20'' in a laboratory stable environment, not including mobility, can be obtained with this NetBox specific configuration.

In the case of jamming applied simultaneously to both primary and secondary radio links then, the communication is permanently lost.

7. General conclusion

This deliverable D3.4 concludes the work performed in Secret workpackage 3, in liaison with WP4. The general objective of this workpackage, led by Ifsttar, with the participation of EHU was to "monitor the electromagnetic environment and to detect electromagnetic attacks". This workpackage was divided in 5 consecutive tasks.

- Task 3.1 concerned the electromagnetic and statistical characterisation of the railway environment in 'normal', i.e. non-jammed, operation conditions.
- Task 3.2 has determined the specifications of the acquisition system to access the quantities to recognize EM attack scenarios identified in WP1.
- Task 3.3 considered the representation space definition of the "normality" and the "non-normality" of the electromagnetic environment.
- Task 3.4 has developed specific models of sub-sets of EM attacks.
- Finally, task 3.5 was dedicated to a proof of concept and evaluation of the developed tools.

This deliverable D3.4 has presented and analysed the results obtained during this task 3.5 lasting from month 25 to month 42 of the project. Two demonstration phases were described and their results were presented and analysed.

Section 1 has explained the purpose of this document.

In section 2, we have presented the waveforms corresponding to intentional jamming that are mainly considered in the project. These waveforms were previously identified and considered in WP1. They can be generated by low-cost, low-power jammers, easily found on the internet.

In a previous deliverable D3.2, we have presented several supervised detection methods that were studied to detect if the railway system is under an electromagnetic attack or not. Following this work, in section 3, we have presented a generic end-to-end jamming sensing method. The hardware and software implementations were described and we have also analysed the results that are provided by such a method. For this analysis, we used a COTS jammer generating the wide band jamming signal

identified in the first section. Effective detections were obtained with these sensors.

Section 4 has introduced our two WP3/WP4 complementary demonstrations. Indeed, jamming real GSM-R signals on board a train or along the track could have intolerable impact on real train operation. Therefore, performing an in situ demonstration could lead to significant railway exploitation problems. For this reason, our Secret demonstrations were oriented a different way.

Section 5 has concentrated on the first Secret demonstration. We selected a video surveillance system whose video signal is transmitted over radio, up to a control centre.
Jamming signals can be generated on demand, in the vicinity of the receivers.
Two different radio communication systems were used. One operating WiFi, at 2.4 GHz and one operating WiMAX, at 5.6 GHz. Both could be separately jammed.
These telecommunications standards and their technical characteristics relevant to our study were analysed. Considering these standards specifications, the detection methods previously presented in deliverables D3.2 and D3.3 were refined.
Five Secret built sensors were realised and presented. They are implemented using either a sophisticated signal processing and state-of-the-art hardware platform, either a low-cost approach. A sixth sensor is a commercial low-cost equipment used as a technical reference. As its characteristics are not very well detailed into the accompanying documentation, it was evaluated in laboratory.
For the demonstrations purpose, specific graphical user interfaces were developed to facilitate the analysis of the EVM and spectral space data.
The sensors were interfaced with the acquisition system using a common database. This makes it possible to write and read sequentially data by all the equipment connected to the database.
The different decision making algorithms implemented to process the raw data received by the acquisition system and provided by the different sensors were presented.
Finally, the obtained results were analysed and a conclusion was drawn in the form of a table. We concluded that, using the prototype sensors and their associated signal processing, we can provide an early warning information to the acquisition system. We also concluded that any of our prototype sensor outperforms the low-cost commercial equipment used as a reference.
Such sensing signal processing techniques could now be implemented on low-cost radio techniques like software defined radio platforms to provide easily reconfigurable jamming detection sensors.

Section 6 has presented our second demonstration scenario and its associated results. This second scenario was selected in order to extend the scope of our initial demonstration. By using a railway radio communication representative equipment, i.e. an ALSTOM NetBox and a non-proprietary radio link, i.e. a 3G radio communication, a second and complementary demonstration scenario was setup.
We used the same sensors, jamming and associated signal processing than during the first demonstration. For this demonstrator, we concentrated on timing measurements to identify loss of communication durations in presence of jamming applied on one of the two used radio links. This was selected to evaluate the interest of developing performant sensors able to early and quickly detect jamming conditions.
We concluded on the strong interest to install in railway environments real time detectors associated to effective reactive systems in order to mitigate the jamming effects.

This section concludes the deliverable.

8. References

[1] Mobile and personal communications committee of the Radio Advisory Board of Canada ‘Radio Advisory Board of Canada’ Use of jammer disabler devices for blocking PCS cellular and related services, Available on line at: http:\\www.rabc.ottawa.on.calelfiles/01pub3.pdf

[2] F. Sabath, Threat of electromagnetic terrorism lessons learned from documented IEMI attacks, EuroEM, p. 17, Jul. 2012.

[3] D. V. Giri and F. M. Tesche, Classification of intentional electromagnetic environments (IEME), IEEE Transactions on Electromagnetic Compatibility, pp. 322-328, 2004.

[4] 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.

[5] R. O. Duda, P. E. Hart et D. G. Stork, Pattern Classification– 2nd edition, John Wiley & Sons, 2000.

[6] S. Mili, D. Sodoyer, V. Deniau, M. Heddebaut, H. Philippe, and F. Canavero. "Recognition process of jamming signals superimposed on GSM-R radiocommunications" In Electromagnetic Compatibility (EMC Europe), 2013 International Symposium on, pp. 45-50, 2013.

[7] M. D. McKinley, K. A. Remley, M. Myslinki, J. S. Kenney, D. Schreurs, B. Nauwelaers, EVM calculation for broadband modulation signals, 64th ARFTG conference, Orlando, Dec. 2004.

[8] R. C. Dixon. 1994. Spread spectrum systems with Commercial Applications (3rd ed.). John Wiley & Sons, Inc., New York, NY, USA.

[9] S.L. Tsao and C.H. Huang. Review: A survey of energy efficient MAC protocols for IEEE 802.11 WLAN. Comput. Commun, Jan. 2011.

[10] Rohde & Schwarz, WLAN 802.11n: From SISO to MIMO; Application Note.

[11] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_5-1/ieee.html.

[12] 802.16e Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems.

[13] Agilent technologies, IEEE 802.11 Wireless LAN PHY Layer (RF) Operation and Measurement Application Note 1380-2.

[14] Rohde & Schwarz, WLAN Measurements, FSW-K91 Test and measurement; User Manual.

[15] Y. Hayakawa, wireless LAN measurement system and dedicated software. Yokogawa-Giho, Yokohawa Electric Corporation, vol. 46 No. 2, pp. 5 1-54,Apr. 22, 2002 (Provided in Japanese and English).

[16] K. Seema, K, Gopi, S. Anand, H. Malati. Experiences with SeaMo: A vertical handoff implementation for heteregeneous wireless networks. Proceedings of the Asia-Pacific Advanced Network Conference 2011.