SPECTRUM INTELLIGENCE FOR INTERFERENCE MITIGATION FOR COGNITIVE RADIO TERMINALS

Kresimir Dabcevic, Muhammad Ozair Mughal, Lucio Marcenaro, Carlo S. Regazzoni

(DITEN, University of Genova, Genoa, Italy)

ABSTRACT

Cognitive Radio (CR) is defined as a radio that is aware of its surroundings and adapts intelligently. While CR technology is mainly cited as the enabler for solving the spectrum scarcity problems by the means of Dynamic Spectrum Access (DSA), perspectives and potential applications of the CR technology far surpass the DSA alone. For example, cognitive capabilities and on-the-fly reconfiguration abilities of CRs constitute an important next step in the Communication Electronic Warfare (CEW). They may enable the jamming entities with the capabilities of devising and deploying advanced jamming tactics. Analogously, they may also aid the development of the advanced intelligent self-reconfigurable systems for jamming mitigation. This work outlines the development and implementation of the Spectrum Intelligence algorithm for Radio Frequency (RF) interference mitigation. The developed system is built upon the ideas of obtaining relevant spectrum-related data by using wideband energy detectors, performing narrowband waveform identification and extracting the waveforms' parameters. The recognized relevant spectrum activities are then continuously monitored and stored. Coupled with the self-reconfigurability of various transmission-related parameters, the Spectrum Intelligence is the facilitator for the advanced interference mitigation strategies. The implementation is done on the Cognitive Radio coaxial test bed architecture which consists of two Software Defined Radio terminals, each interconnected with the computationally powerful System-on-Module (SoM).

1. INTRODUCTION

As opposed to the legacy radio systems, where the functionalities are for the most part restricted by the deployed hardware components, Software Defined Radios (SDRs) provide reconfigurability of most of their parameters through software changes run on the programmable processors - Field Programmable Gate Arrays (FPGAs) or Digital Signal Processors (DSPs). Originally introduced by Mitola in 1991, SDR is nowadays becoming a dominant design architecture for wireless systems. Cognitive Radio (CR) is usually built on a SDR platform, and is further embodied with awareness and self-adapting capabilities. This, however, inherently brings along higher implementation complexity and the needs for even more powerful computational resources.

SDRs and CRs [1] have received particular interest from the wireless communication research community as potential solutions to spectrum underutilization problems. For these purposes, a variety of Dynamic Spectrum Access (DSA) techniques have been proposed and investigated. These may be categorized under the three models: Dynamic Exclusive Use, Open Sharing, and Hierarchical Access Models [2]. Opportunistic Spectrum Access (OSA) is a form of the Hierarchical Access Model, where unlicensed CRs (secondary users) are allowed to utilize the spectrum as long as licensed (primary) users' communication is protected. In order to access the spectrum opportunistically, secondary users need to be able to acquire the spectrum occupancy information. Three methods enabling the spectrum occupancy inference are generally adopted: spectrum sensing, geolocation/database and beacon signals. Among them, various spectrum sensing techniques such as energy detection [3, 4], feature detection [5] and matched filters [6] were given the most attention up to date.

However, the potentials of SDR and CR paradigms are not necessarily restricted to the application of DSA. Seamless transition between the existing communication solutions, higher interoperability between different standards and flexibility in waveform selection all impose themselves as the viable reasons for research and development of the SDR and CR concepts.

In this work, we focus on some of the impacts that the SDR/CR technology brings to the Communication Electronic Warfare (CEW) domain. CEW systems [7] focus on intercepting or denying the communication on the target systems (electronic attack) [8], or taking actions aimed at preventing the electronic attacks from successfully occurring (electronic defense). A multitude of ways with respect to how on-the-fly reconfiguration capabilities coupled with the learning and self-adaptive potentials of the CR technology may aid both the attacking and the defending side can be imagined [9]. Deploying energy detection spectrum sensing may embody the attacker with the ability to monitor the target transmitter's transmission frequency, estimate the target receiver's signal strength and calculate the signal strength necessary to efficiently jam the communication. Performing feature detection

spectrum sensing may allow the attacker to infer even more of the parameters of the target transmitter, such as deployed modulation type or coding mechanism. Subsequently, it may use these inferences to deploy jamming tactics with higher probability of success rate, e.g. by taking advantage of the fact that different modulation techniques are characterized by different levels of resilience to interference. Finally, the attacker may use learning techniques to observe and learn the transmitter's patterns, such as the deployed frequency hopping or power allocation schemes. Analogously, similar benefits may be provided to the defending side.

This work focuses on the electronic defense part of the CEW. It presents ideas, development and implementation aspects of the Spectrum Intelligence algorithm for Radio Frequency (RF) interference mitigation. The concept is built on the enabling technologies of spectrum sensing, waveform analysis, Temporal Frequency Maps[1], and self-reconfigurability potentials of the SDR/CR technology.

Along the way, we acknowledge and address some of the challenges faced when porting the algorithms to the real-life SDR/CR platform, and propose practical solutions for the identified problems.

The remainder of the paper is organized as follows: section 2 describes the enabling technologies and concepts for the Spectrum Intelligence algorithm, as well as the concepts and functionalities related to the algorithm itself. The SDR/CR platform used for porting the developed algorithms, along with the identified issues and proposed solutions is described in section 3. Performance of several crucial functionalities of the algorithm is evaluated in section 4, whereas conclusions and the roadmap are presented in section 5.

2. SPECTRUM INTELLIGENCE

The principal idea behind the Spectrum Intelligence algorithm consists of continuously monitoring relevant RF spectrum activities, identifying potential threats to the communication, and taking proactive measures to ensure communication robustness and secrecy. For doing so, the algorithm relies on the reliable spectrum sensing mechanism, correct identification and extraction of the relevant parameters, and secure software unsubjected to tampering. The functional process of the Spectrum Intelligence algorithm may be represented in the form of the Cognitive Cycle, as shown in Figure 1.

Sensing is performed periodically, either by taking a quiet or active approach, for the frequency band of interest.

Then, *data processing* takes place. Parsed data is time aligned if needed, and transformed into frequency domain by performing Fast Fourier Transform (FFT). Thresholding is then performed with the aim of discarding the background noise, and keeping only the FFT bins corresponding to actual

[1]We are intentionally creating a distinction between the Temporal Frequency Maps, and the similar but more advanced concept of Radio Environment Maps [10].

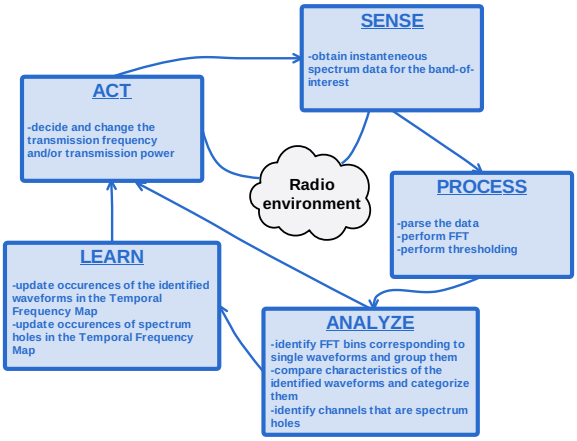

Fig. 1: Cognitive cycle representing the Spectrum Intelligence algorithm

signals. This corresponds to solving the decision problem between the following two hypotheses [11]:

$$Y(n) = \begin{cases} W(n) & H_0 \\ X(n) + W(n) & H_1 \end{cases} \quad (1)$$

where $Y(n)$, $X(n)$ and $W(n)$ are the received signals, transmitted signals and noise samples, respectively, H_0 is the hypothesis corresponding to the absence of the signal, and H_1 is the hypothesis corresponding to the presence of the signal.

Finding the appropriate threshold is the principal challenge of any energy detection scheme. The most common approaches are the Constant Detection Rate (CDR) and Constant False Alarm Rate (CFAR) detectors, where threshold is set adaptively depending on the SNR regime and the characteristics of the sensed wideband signal. However, it should be noted that even in adaptive thresholding, presence of interference may confuse the energy detector [12].

In CEW domain, it is reasonable to assume relatively low spectrum utilization - namely, more often than not there will only be a limited number of actual narrowband signals (either "friendly" or "potentially malicious") in the scanned wideband signal at any time instance. For this purpose, it is sufficient to implement a suboptimal thresholding algorithm, where CFAR or CDR performance is not necessarily achieved. Namely, practical experience has shown that threshold $\hat{\lambda}$ may be adaptively set based only on the mean value of the magnitudes of the scanned wideband signal, as:

$$\hat{\lambda} = 2 \cdot \frac{1}{n} \sum |Y(n)| \quad (2)$$

This step concludes the energy detection.

Let us assume that as a result of the thresholding process, N frequency bins are identified. For a system where M actual signals ($N > M$) are present, $N - M$ frequency bins would

incorrectly be classified as signals. Then, simple thresholding would result in the false alarm rate of $\frac{N-M}{N}$.

For this reason, frequency bins corresponding to the same signal need to be grouped together. For the ideal case (generic signals in high-SNR environments), the simplest approach consists of grouping consecutive samples together and classifying them as single waveforms. However, in most practical situations, some frequency bins may have erroneous magnitude values as a result of imperfect sampling and would thus be discarded during the thresholding phase. For this purpose, maximum acceptable distance (in Hz) between the two samples belonging to the same waveform is defined, and is a function of the frequency resolution of the FFT as given by:

$$d_{MAX} = K \cdot d_f. \tag{3}$$

Here, K is the estimate of a number of consecutive samples that could be erroneously disregarded, and d_f is the frequency resolution of the FFT, defined as:

$$d_f = \frac{2 \cdot f_{max}}{N_S}, \tag{4}$$

where f_{max} is the maximum resolvable frequency (which in case of Nyquist sampling equals to half of the sampling frequency), and N_S is the number of samples acquired during the sampling process.

Figure 2 illustrates the difference between the original transmitted signal (2(a)), sensed FFT bins (2(b)), and estimated signal after performing thresholding/bin grouping (2(c)).

Next, the *waveform analysis* is performed, i.e. for each of the identified narrowband waveforms, relevant parameters are extracted. These parameters include waveforms' respective center frequencies, bandwidths and maximum values of their magnitudes. It is assumed that the algorithm has an access to a database containing pre-defined parameters of the "friendly" and/or "potentially malicious" waveforms in the system. Then, parameters of the identified waveforms in the system are compared to the parameters from the database, eventually resulting in classification of each waveform as either "friendly" or "potentially malicious".

The considered method for waveform analysis is computationally inexpensive, and is suitable for analysis in systems with low frequency resolution. However, there is a tradeoff between the lightweight nature of the algorithm and the limitations it imposes, which are as follows:

1. Relatively high probability of misclassification / misdetection compared to more advanced waveform analysis methods in systems with higher frequency resolution, as a result of a limited number of analyzed parameters.

2. The need for a-priori knowledge of the expected maximum values of the magnitudes, which in real-life situations may not always be feasible.

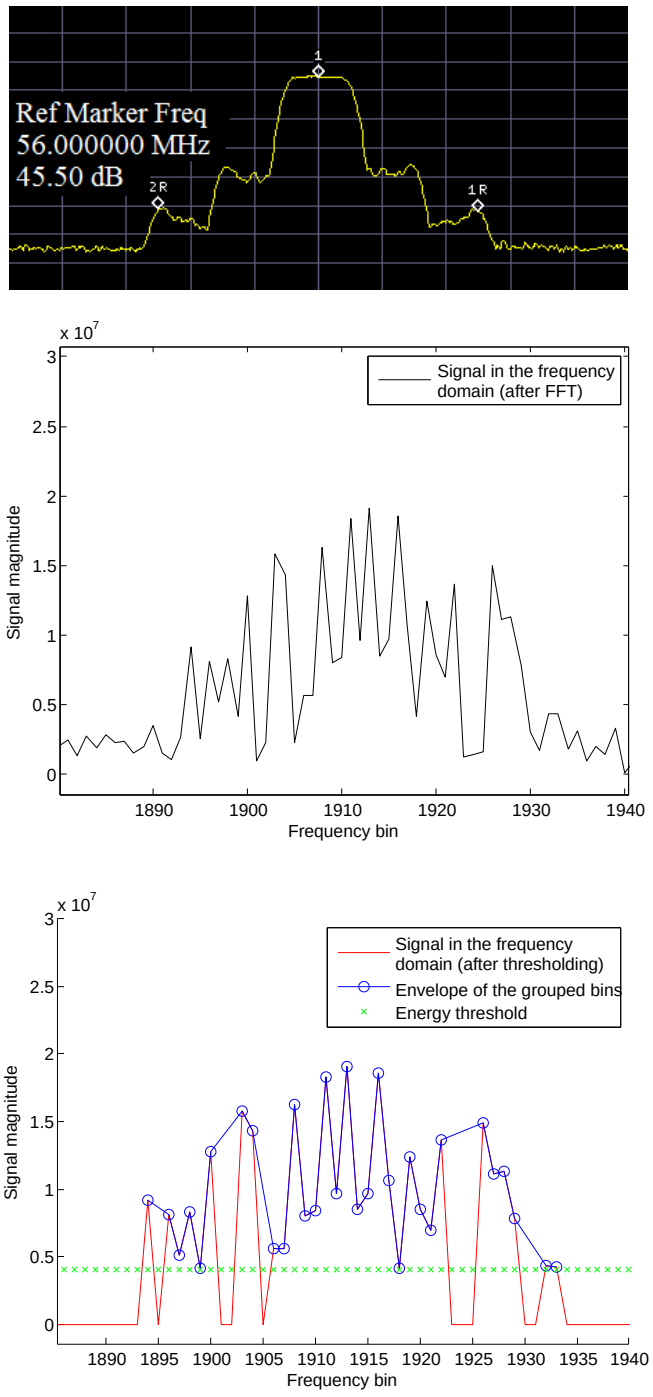

Fig. 2: Signal: transmitted - maximum hold (a), sensed (b), after thresholding and bin grouping (c)

3. Vulnerability against adversaries able to refine their transmission-related parameters in order to mimick "friendly" users (the so-called User Emulation Attackers [13]).

Alternative, computationally more expensive waveform analysis techniques include cross-correlation in time domain; more comprehensive Statistical Signal Characterization (SSC) methods [14]; modulation classification methods [15]; and cyclostationary detectors [5]. These are not analyzed within this work, however they all impose themselves as viable future research topics.

Besides waveform identification and classification, the system also recognizes instantaneous spectrum holes. We define a spectrum hole as the channel where the magnitudes of all of the corresponding FFT bins are below the energy threshold.

The algorithm next accesses the Temporal Frequency Map, where previous occurrences of spectrum activities are stored. The Temporal Frequency Map is a $n \times 3$ matrix that keeps track of the number of occurrences of "friendly" waveforms, "potentially malicious" waveforms and spectrum holes for each of the n channels-of-interest, as illustrated in Table 1.

Table 1: Temporal Frequency Map

Spectrum activity/CHANNEL	1	2	...	n
Friendly	$m_{F/1}$	$m_{F/2}$		$m_{F/n}$
Potentially malicious	$m_{PM/1}$	$m_{PM/2}$		$m_{PM/n}$
Spectrum hole	$m_{SH/1}$	$m_{SH/2}$		$m_{SH/n}$

In each cycle, previous values are updated with the newly acquired and processed information. This corresponds to the *learning* phase of the Cognitive cycle. Temporal forgiveness is implemented within the algorithm, i.e. spectrum activities corresponding only to the last k spectrum readouts are taken into account while making future decisions. This reduces the probability of data becoming obsolete, at the expense of the lower amount of accessible information.

Finally, based on the processed spectrum information, current transmission parameters (channel and power) and the history obtained from the Temporal Frequency Map, the CR may decide to *act* in order to improve its chances of reliable transmission. The actions constitute of proactively changing the transmission frequency (channel surfing), or the transmission power whenever a threat has been detected. A system is considered "under threat" when a "potentially malicious" waveform has been identified on the channel close to the channel currently used for transmission. The new channel for the transmission is then chosen according to (5).

$$c_{t+1} \in (c_t = SH \mid (X(c_t) = min). \tag{5}$$

This means that the new channel c_{t+1} is selected among all the channels c_t that are currently spectrum holes, such that the $X(c_t)$ is minimum. $X(c_t)$ represents the expected channel reliability, defined as (6).

$$X(c_t) = k^2 \cdot m_{PM/c_t} + (k+1) \cdot m_{F/c_t} - m_{SH/c_t}, \tag{6}$$

where m_{PM/c_t}, m_{F/c_t} and m_{SH/c_t} represent the numbers of occurrences of the "potentially malicious" waveforms, "friendly" waveforms and spectrum holes on the channel c_t over the last k steps, respectively. The coefficients k^2 and $(k+1)$ are assigned in order to give highest priority of action to avoiding channels with history of occurrences of "potentially malicious" waveforms, followed by the channels with history of occurrences of "friendly" waveforms.

The new transmission power is chosen according to (7).

$$P_{t+1} \in P \mid P_R > 10log_{10}\hat{\lambda} + 3dB. \tag{7}$$

Algorithm 1 provides the pseudocode demonstrating processes related to the Spectrum Intelligence algorithm.

Algorithm 1 Spectrum Intelligence pseudocode

function SPECTRUM INTELLIGENCE
  Initialize all channel states to "free"
  Sample the wideband signal $\rightarrow N_S$ *amplitude values*
  Data parsing $\rightarrow N_S = 2^x$ *amplitude values*
  Perform FFT $\rightarrow \frac{N_S}{2}$ *frequency bins with magnitudes* M
  Calculate mean value of $M \rightarrow M_{mean}$
  Based on M_{mean}, set the energy threshold $\rightarrow \hat{\lambda}$
  for $i = 1 to \frac{n_s}{2}$ **do** (For each frequency bin)
    if $M(i) > \hat{\lambda}$ **then**
      Bin i belongs to the signal
      Change channel state of bin i to "occupied"
      if any of $M(i-K)$:$M(i-1) > M_T$ **then**
        Group these bins as a single waveform
      end if
    end if
  end for
  Extract parameters of identified waveforms $\rightarrow$ *bandwidth*, *center frequency*, *maximum* M
  Compare parameters to the database $\rightarrow$ *waveform is either "friendly" or "potentially malicious"*
  Update Radio Frequency Map
  If "potentially malicious" waveforms are near the current operating channel, choose new TX frequency/power
end function

3. IMPLEMENTATION ON THE CR TEST BED

The proposed algorithm was implemented on the SDR/CR coaxial test bed architecture. Compared to the over-the-air

implementation, coaxial test bed exhibits several important advantages:

- Possibility to set accurate and stable RF levels,
- Repeatability of the experiments without the uncertainties characteristic to wireless transmission,
- Possibility to connect test instruments and generators to one or more branches,
- Avoiding regulatory issues related to transmitting outside of the Industrial, Scientific and Medical (ISM) frequency bands.

Test bed consists of two Software Defined Radio (SDR) SWAVE HandHeld (HH) terminals [16], each interconnected with the computationally powerful System-on-Module (SoM) embodied with a Digital Signal Processor (DSP) and a Field Programmable Gate Array (FPGA). Inbetween, a dual directional coupler is placed. Vector signal generator allows for injecting noise/interference to the system, whereas spectrum analyzer provides reliable monitoring of the relevant RF activities in real-time. Block diagram of the test bed architecture is provided in Figure 3.

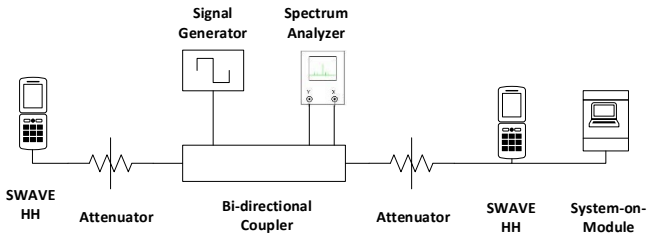

Fig. 3: CR test bed block diagram

SWAVE HH is a fully functional SDR terminal operable in Very High Frequency (VHF) and Ultra High Frequency (UHF) bands, capable of hosting a multitude of both legacy and new waveforms. Additionally, it provides support for remote control of its transmit and receive parameters via the Simple Network Management Protocol (SNMP). All of the signal processing is delegated to the SoM. Connection between the HH and SoM is achieved through Ethernet and serial ports. Ethernet is used for the remote control of the HH's parameters, using SNMP v3. For the purposes of the Spectrum Intelligence algorithm, relevant remotely controllable parameters are operating channel and transmission power. Serial port is used to transfer raw spectrum data from the HH to SoM. The interfaces are illustrated in Figure 4, and the actual implementation in Figure 5. Full details on the test bed architecture may be found in [17].

Here follows a description of the spectrum sensing process based on the HH's wideband front end architecture (Figure 6). HH's 14-bit Analog-to-Digital-Converter (ADC) performs sampling at 250 Msamples/s. Every 3 seconds, a burst

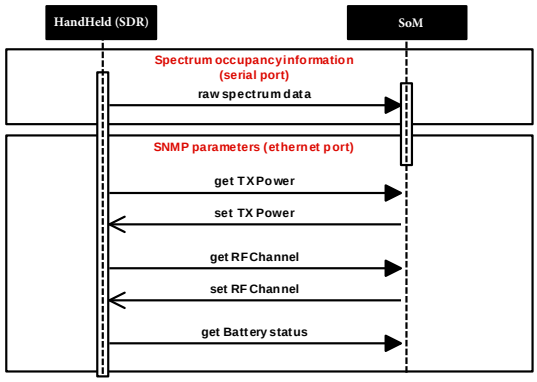

Fig. 4: Interfaces HandHeld-SoM

Fig. 5: Implementations of HandHeld and SoM

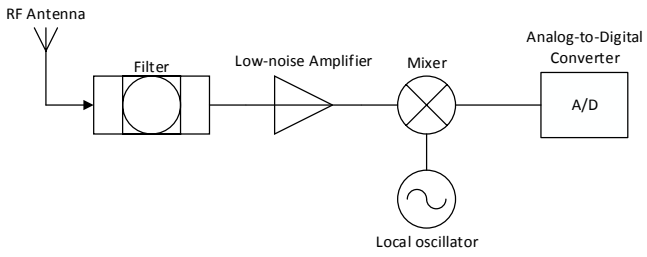

Fig. 6: HandHeld's wideband RF front end architecture

of 8192 consecutive samples is buffered, and then outputted over the serial port at 115200 bauds to the SoM. There, the samples, corresponding to 120 MHz around the center carrier frequency of the radio, are parsed, transformed into the frequency domain using the Fast Fourier Transform (FFT), and subsequently analyzed by the implemented energy detector. Alternatively, in order to increase the frequency resolution of the FFT bins, several consecutive spectrum bursts may be FFT-ed, averaged and analyzed together. The spectrum sensing and the Spectrum Intelligence as a whole is a quite process, i.e. throughout the process, HH is able to transmit/receive data. Controlled environment achieved by the coaxial implementation allows us to assume high coherence time of the analyzed frequency band, i.e. while performing the averaging of consecutive spectrum readouts, temporal variability of the channel may be disregarded. We acknowledge, however, that in case of the over-the-air transmission, nature of the wireless medium would not allow us to make such assumption. In order to obtain higher FFT frequency resolutions, necessary modifications to the equipment would include increasing the buffer size on the HH, and finding ways to transfer spectrum data at higher baud rate than is currently supported. Alternatively, appropriate techniques that estimate the temporal variability of the channel would need to be deployed.

The FFT-ed data is then further analyzed by the Spectrum Intelligence algorithm, as explained in Section 2. The output of the algorithm is the transmission frequency and transmission power to be deployed in the next cycle. These values are written to the .xml file at the end of the Spectrum Intelligence cycle.

As previously mentioned, HH provides support for reconfigurability of its transceiving parameters by the means of the SNMP v3. The implementation is done in the following way: whenever a new value is written into the .xml file representing the new transmission frequency/power, the algorithm running on the SoM intreprets it as the SNMP command that needs to be invoked. Each SNMP command (`SET_RFchannel` or `SET_TXpower`) is characterized by the corresponding unique Object IDentifier (OID) and the new value of the parameter. OIDs and the respective values that each object can take are stored in the Management Information Base (MIB) on the HH. Once that the HH receives the SET request, it accesses the MIB, checks whether the requested value of the object is defined in MIB and, if so, changes the corresponding parameter. This finishes one cycle of the Spectrum Intelligence algorithm. Change of the transmission parameters occurs in every cycle in which the "under threat" alarm has been triggered.

4. EXPERIMENTAL VALIDATION

Performance of the overall algorithm depends mainly on the accuracy of the energy detection and waveform classification phases. In order to evaluate the performance of these functionalities, a set of experiments is performed using the test bed architecture.

SelfNET Soldier Broadband Waveform (SBW) [16], representing the "potentially malicious" waveform, is continuously transmitted on the fixed carrier frequency. SBW is a digital waveform with 1.25 MHz bandwidth, operable in VHF (30 MHz-88 MHz) and UHF (256 MHz-512 MHz) frequency bands. When operating in VHF, direct conversion principle is utilized, and the frequency band scanned is always 0-120 MHz. When operating in UHF, superheterodyne principle is used, and the frequency band scanned depends on the center carrier frequency f_c of the radio - namely, analyzed band is $[f_c - 35, f_c + 85]$ MHz. Vector signal generator is used to create and inject the "friendly" waveforms into the channel, emulating friendly communication. In addition, for the ease of analysis, all other sensed recognized signals that are not classified as "potentially malicious" are classified as "friendly". Hence, the database contains only the parameters of the "potentially malicious waveform" - i.e. its bandwidth and expected maximum magnitude.

For the experiments, we utilize the VHF transmission band where the radios are operable, meaning that the spectrum sensing is performed for the frequency band of 0-120 MHz. SBW signal representing the "potentially malicious" waveform is transmitted at the center carrier frequency of 61 MHz (first 100 spectrum bursts) and 71 MHz (second 100 spectrum bursts), always with the constant transmission power. These results are then aggregated and analyzed. Besides the SBW signal, a number of other signals from the environment are successfully sampled, e.g. FM radio transmission in the frequency band of 88-108 MHz. Figure 7(a) shows an example of the scanned wideband signal for 1 sensing burst (29.3 kHz frequency resolution). Figures 7(b) and 7(c) show the difference in frequency resolution between 1 burst and 5 consecutive averaged bursts (5.86 kHz frequency resolution).

Ideally, waveform analysis should classify only the SBW waveform as the "potentially malicious" waveform in every analysis cycle (true positives). However, the analysis procedure will occasionally erroneously classify other waveforms as "potentially malicious" (false positives).

These classification results are directly dependent on the following factors:

- Energy detection threshold, $\hat{\lambda}$ - inappropriately low threshold may result in grouping together many adjacent bins (some of which actually corresponding to noise) as single waveforms, consequently increasing the estimated bandwidths of these waveforms.

- Estimated number of consecutive samples that could be erroneously disregarded, K - overly low K may result in single waveforms being erroneously recognized as different waveforms on adjacent frequencies; overly high

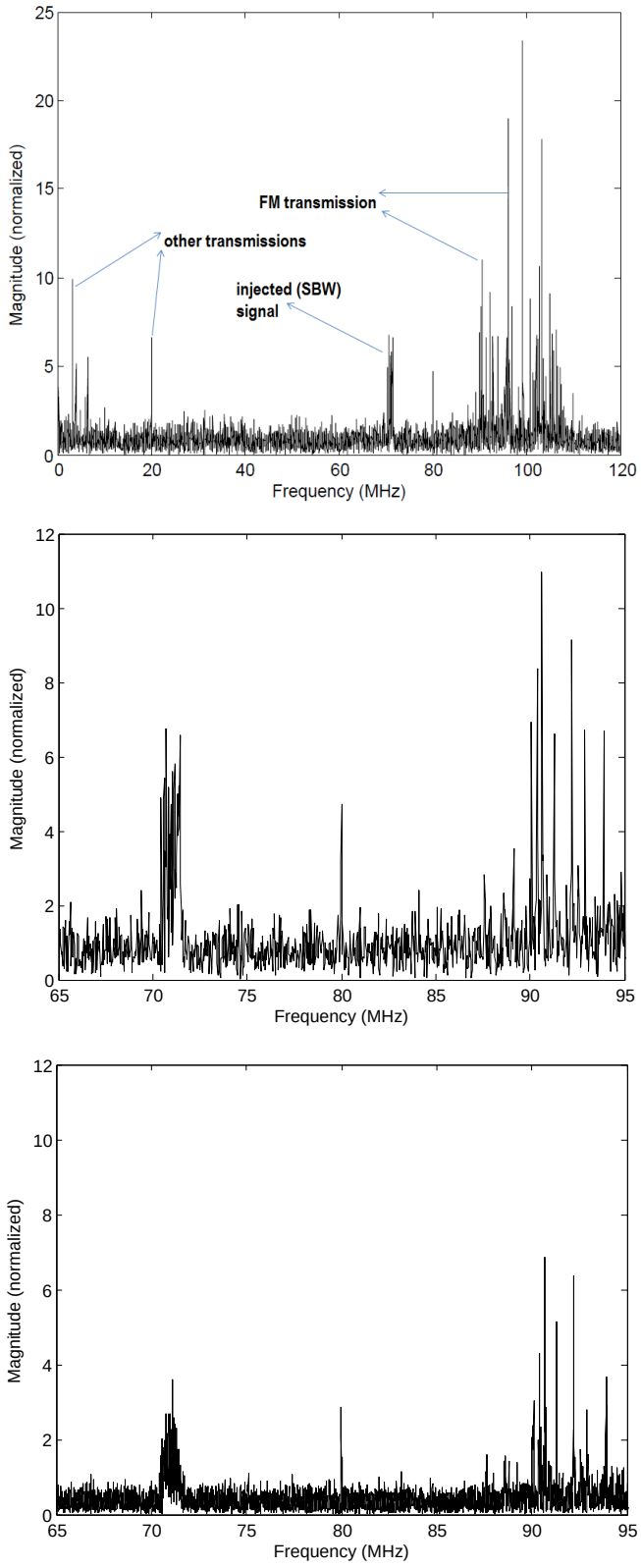

Fig. 7: Signal: wideband sensed - 1 analyzed burst (a), zoomed in - 1 analyzed burst (b), zoomed in - 5 analyzed bursts (c)

K may result in waveforms on adjacent frequencies being erroneously grouped as single waveforms.

- Similarity in the parameters between the analyzed waveform and other scanned waveforms present in the communication system.

- Level of tolerance on the analyzed parameters (e.g. 20% tolerance on bandwidth means that for SBW, whose bandwidth is 1.35 MHz, all scanned waveforms whose bandwidth falls between [1.08,1.62] MHz will be classified as the SBW waveform) - higher tolerance will increase the probability of both true and false positives.

- Frequency resolution, directly stemming from the number of averaged consecutive bursts.

The first two points are defined according to (2) and (3) respectively, with $K = 3$. In the analyzed system, all scanned signals have significantly narrower bandwidths than the analyzed (SBW) signal, as can be seen from Figure 7(b). Hence, we focus our analysis on the influence of the last two points.

First, waveform analysis is performed using only the estimated bandwidths of the scanned waveforms. Level of tolerance varies between 10% and 30%, and number of consecutive analyzed bursts varies from 1 to 10. Results are summarized in the form of the confusion matrix in Table 2.

Here, ”true positives” refer to the correctly classified instances of the ”potentially malicious” (SBW) waveform. ”False positives” are all other (”friendly”) waveforms erroneously classified as ”potentially malicious”. Whereas it could have been foreseen that the rate of true positives increases significantly with frequency resolution (number of averaged bursts), the rate of increase of false positives may

Table 2: Confusion matrix when only the estimated bandwidths are used

		Parameter tolerance (%)		
No. of bursts		*10*	*20*	*30*
1	*True positives (200 runs)*	*55*	*92*	*130*
	False negatives (200 runs)	*145*	*108*	*70*
	False positives (200 runs)	*0*	*4*	*9*
3	*True positives (66 runs)*	*48*	*59*	*61*
	False negatives (66 runs)	*18*	*7*	*5*
	False positives (66 runs)	*14*	*20*	*27*
5	*True positives (40 runs)*	*36*	*40*	*40*
	False negatives (40 runs)	*1*	*0*	*0*
	False positives (40 runs)	*20*	*26*	*34*
10	*True positives (20 runs)*	*18*	*20*	*20*
	False negatives (20 runs)	*2*	*0*	*0*
	False positives (20 runs)	*16*	*23*	*52*

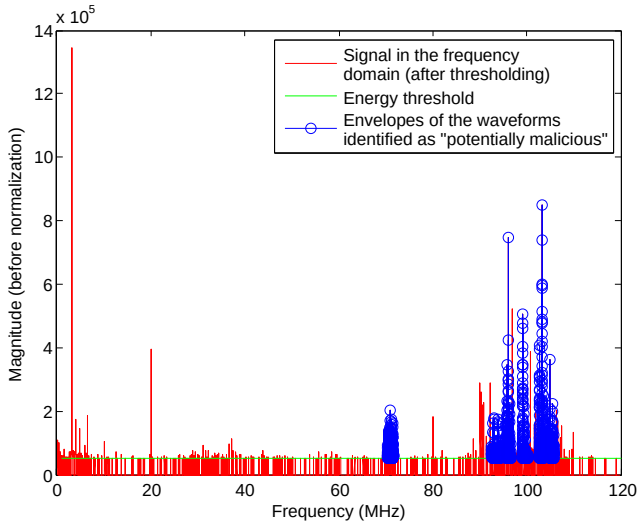

Fig. 8: Occurrences of false positives - 10 consecutive analyzed bursts, parameter tolerance 30%

come as a surprise. Figure 8 proffers a good explanation for this occurrence:

Here, instances of both the correct detection (waveform at 71 MHz) and of five false detections (waveforms at approximately 94, 96, 99, 103 and 105 MHz) are present. False detections are caused by several factors: imperfect sampling and low sampling time throughout analyzed sampling windows cause that the FFT bins appear at slightly different frequencies (especially for the narrowband FM radio signals). Some of these values then superimpose, making their respective magnitudes satisfy the threshold $\hat{\lambda}$. Adjacent ($K = 3$) frequency bins that are over the threshold are grouped together and analyzed as single waveforms. Occasionally, these "waveforms" will have estimated bandwidth that falls within the tolerance of the analyzed (SBW) waveform, in turn triggering the false detection.

This may partially be solved by imposing higher constraint on $\hat{\lambda}$ or lower constraints on K. Alternatively, analyzing other waveform parameters (when available) may provide even better analysis results. In the second step, waveform analysis is performed using both the information of the estimated bandwidth and the maximum magnitude for the scanned waveforms. Table 3 shows the improvements with respect to the reduced number of false positives, at the expense of the reduced number of identified true positives.

We acknowledge that, whereas information on the adversaries' transmission powers may often not be known a-priori in real-life scenarios, they might be known for some "friendly" signal. Then, with the appropriate channel estimation techniques and the information on the "friendly" waveforms' geographical positions, expected scanned power or magnitude may be predicted (with a certain tolerance).

Table 3: Confusion matrix when both the estimated bandwidths and the estimated magnitudes are used

		Parameter tolerance (%)		
No. of bursts		*10*	*20*	*30*
1	*True positives (200 runs)*	*32*	*85*	*123*
	False negatives (200 runs)	*168*	*115*	*77*
	False positives (200 runs)	*0*	*0*	*0*
3	*True positives (66 runs)*	*35*	*44*	*54*
	False negatives (66 runs)	*31*	*22*	*12*
	False positives (66 runs)	*0*	*0*	*0*
5	*True positives (40 runs)*	*34*	*36*	*37*
	False negatives (40 runs)	*6*	*4*	*3*
	False positives (40 runs)	*0*	*0*	*0*
10	*True positives (20 runs)*	*17*	*20*	*20*
	False negatives (20 runs)	*3*	*0*	*0*
	False positives (20 runs)	*0*	*0*	*0*

Finally, we measure the execution time of the Spectrum Intelligence algorithm for varying numbers of analyzed bursts. The results are shown in Figure 9.

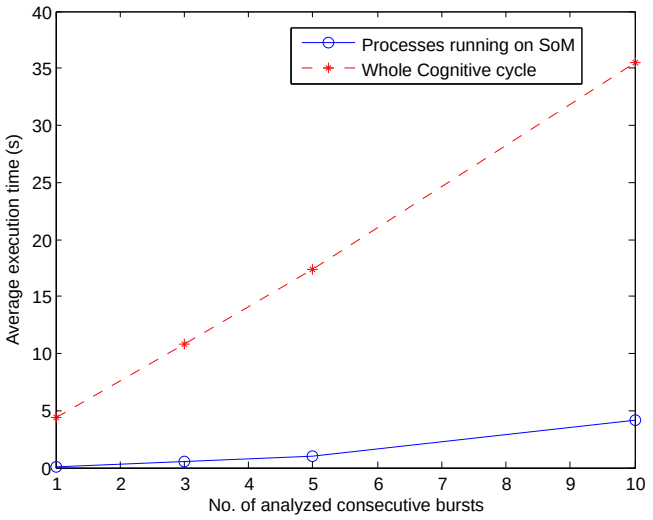

Fig. 9: Average execution times of the Spectrum Intelligence algorithm

Full blue line shows the computational time of the Process-Analyze-Learn-Decide phase of the Spectrum Intelligence, corresponding to all the processes that are running on the SoM. Computational times of the whole cognitive cycle, including the sensing time and the time needed to deploy the appropriate SNMP command on the radio are represented by the dashed red line. Sensing time takes approximately 3 seconds per burst, whereas invoking and executing the SNMP command takes approximately 1.3 seconds. In case of channel surfing, additional frequency settling time of the HH is

negligible, and corresponds to 40 microseconds.

The performance of the Spectrum Intelligence algorithm as a whole depends primarily on the jamming tactics deployed by the adversaries, as well as on the system parameters such as number of available channels for frequency hopping, and successful classification of these channels as spectrum holes depending on the occurrences of "friendly"/other waveforms in the system. Against naive narrowband jamming entities that change their transmission frequency slowly, Spectrum Intelligence proffers next to a foolproof strategy for jamming evasion. However, against more advanced opponents that are able to adapt their tactics as fast as the Spectrum Intelligence algorithm, the performance is yet to be evaluated.

5. CONCLUSIONS AND FUTURE WORK

In the paper, we have presented the ideas, development and implementation aspects of the Spectrum Intelligence algorithm for Interference Mitigation. The algorithm is based on the learning capabilities and the on-the-fly reconfiguration of the transmission-related parameters characteristic to Cognitive Radio technology. Implementation of the algorithm was done on the SWAVE HandHeld - a military Software Defined Radio - interconnected with the computationally powerful System-on-Module. Performance of several crucial functionalities of the algorithm was evaluated and presented. Main identified challenges included: finding optimal algorithm for adaptive energy detection thresholding; optimal set of features for waveform comparison and classification, and reasonable execution time.

Future work will involve further work on the optimal adaptive thresholding, as well as the more advanced waveform classification techniques. Testing of all of the implemented functionalities will be done against emulated Cognitive Radio jammers able to deploy advanced jamming tactics.

Acknowledgements

This work was partially developed within the nSHIELD project (http://www.newshield.eu) co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems.

The authors would like to thank Selex ES and Sistemi Intelligenti Integrati Tecnologie (SIIT) for providing the equipment for the test bed, and the laboratory premises for the test bed assembly. Particular acknowledgments go to Virgilio Esposto of Selex ES and to Gabriele Dura of University of Genova, for providing expertise and technical assistance.

6. REFERENCES

[1] J. Mitola and Jr. Maguire, G.Q., "Cognitive radio: making software radios more personal," *Personal Communications, IEEE*, vol. 6, no. 4, pp. 13–18, 1999.

[2] Qing Zhao and B.M. Sadler, "A survey of dynamic spectrum access," *Signal Processing Magazine, IEEE*, vol. 24, no. 3, pp. 79–89, May 2007.

[3] M. O. Mughal, L. Marcenaro, and C. S. Regazzoni, "Energy detection in multihop cooperative diversity networks: An analytical study," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[4] G. Bartoli, D. Marabissi, R. Fantacci, L. Micciullo, C. Armani, and R. Merlo, "Performance evaluation of a spectrum-sensing technique for ldacs and jtids coexistence in l-band," in *Proceedings of SDR'12 - WinnComm-Europe*, June 2012, pp. 17–23.

[5] A. Tkachenko, D. Cabric, and R.W. Brodersen, "Cyclostationary feature detector experiments using reconfigurable bee2," in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, April 2007, pp. 216–219.

[6] S. Kapoor, S.V.R.K. Rao, and G. Singh, "Opportunistic spectrum sensing by employing matched filter in cognitive radio network," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, June 2011, pp. 580–583.

[7] R. Poisel, *Introduction to Communication Electronic Warfare Systems*, Artech House, Inc., Norwood, MA, USA, 2 edition, 2008.

[8] F. Delaveau, A. Evesti, J. Suomalainen, and N. Shapira, "Active and passive eavesdropper threats within public and private civilian wireless-networks - existing and potential future countermeasures - a brief overview," in *Proceedings of SDR'13 -WinnComm-Europe*, June 2013, pp. 11–20.

[9] K. Dabcevic, A. Betancourt, C.S. Regazzoni, and L. Marcenaro, "A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, 2014, pp. 8208–8212.

[10] H.B. Yilmaz, T. Tugcu, F. Alagoz, and S. Bayhan, "Radio environment map as enabler for practical cognitive radio networks," *Communications Magazine, IEEE*, vol. 51, no. 12, pp. 162–169, December 2013.

[11] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. on Commun.*, vol. 55, no. 1, pp. 21–25, 2007.

[12] D. Cabric, S.M. Mishra, and R.W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, Nov 2004, vol. 1, pp. 772–776 Vol.1.

[13] N.T. Nguyen, Rong Zheng, and Zhu Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification," *Signal Processing, IEEE Transactions on*, vol. 60, no. 3, pp. 1432–1445, 2012.

[14] H.L. Hirsch, "Statistical signal characterization - new help for real-time processing," in *Aerospace and Electronics Conference, 1992. NAECON 1992., Proceedings of the IEEE 1992 National*, May 1992, pp. 121–127 vol.1.

[15] W. M. Meleis, *Signal detection and digital modulation classification-based spectrum sensing for cognitive radio*, Ph.D. thesis, Northeastern University, Boston, Massachusetts, 2013.

[16] SelexES, "Swave hh specifications," 2013.

[17] K. Dabcevic, L. Marcenaro, and C. S. Regazzoni, "Spd-driven smart transmission layer based on a software defined radio test bed architecture," in *Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems*, 2014, pp. 219–230.