Advanced coexistence technologies for radio optimisation in licensed and unlicensed spectrum

(ACROPOLIS)

Document Number D14.2

Description of validation/certification challenges for Software Defined Radio and Cognitive Radio

Contractual date of delivery to the CEC:	30/09/2012
Actual date of delivery to the CEC:	30/09/2012
Project Number and Acronym:	257626 - ACROPOLIS
Editor:	Gianmarco Baldini (JRC)
Authors:	Gianmarco Baldini (JRC), Oliver Holland (KCL), Aimilia Bantouna (UPRC), Andreas Polydoros (IASA)
Participants:	UPRC, KCL, JRC, EADS, IASA
Workpackage:	WP14
Security:	RE
Nature:	Report
Version:	1.0
Total Number of Pages:	34

Abstract:

Validation and certification of Software Defined Radio (SDR) and Cognitive Radio (CR) presents new challenges in comparison with the testing of conventional communication systems. Verification is usually defined as the activity of checking that a product, service, or system (or portion thereof, or set thereof) meets a set of initial design requirements, specifications, and regulations. The capability of SDR to download and activate new software modules and waveforms poses new challenges for the certification process because communication behaviour and parameters can change after market deployment. In a similar way, CR devices can transmit in a wide range of frequencies and they can change their emission parameters based on the local spectrum environment. This flexibility may require new validation and testing procedures, which this Deliverable discusses. Moreover, because CR devices might increase the risk of harmful interference to existing wireless infrastructures and radio communication devices, this Deliverable also describes interference mitigation techniques which can be used in post-market deployment scenarios.

Keywords:
SDR, CR, validation, testing

Document Revision History

Version	Date	Author	Summary of main changes
0.1	16.06.2011	Gianmarco Baldini (JRC)	Initial structure of the document, ToC developed.
0.2	24.04.2012	Gianmarco Baldini (JRC)	New draft with additional content.
0.3	26.06.2012	Gianmarco Baldini (JRC)	New draft with additional content.
0.4	05.07.2012	Gianmarco Baldini (JRC)	Added new content and adopted new template.
0.5	27.07.2012	Gianmarco Baldini (JRC), Oliver Holland (KCL), Aimilia Bantouna (UPRC)	Added new content after D14.2 PhConference.
0.6	14.08.2012	Gianmarco Baldini (JRC)	New content on mitigation techniques.
0.7	30.08.2012	Gianmarco Baldini (JRC), Oliver Holland (KCL)	Updated after comments.
0.8	05.08.2012	Gianmarco Baldini (JRC), Oliver Holland (KCL), Andreas Polydoros (IASA)	Updated after WP14 PhConference on 4.08.2012.
1.0	28.09.2012	Gianmarco Baldini (JRC)	Finalised document.

Table of Contents

Executive Summary

Demand for services which are dependent upon access to the radio spectrum is rapidly increasing, and new technologies like Software Defined Radio (SDR) and Cognitive Radio (CR) can provide innovative approaches to increase spectrum utilization. Equipment based on SDR and CR technology may have specific features and behaviour in comparison to conventional communication systems. SDR devices might download and activate new software modules (i.e., waveforms) to implement new communication standards after deployment in the field. This behaviour is quite different from conventional wireless communication devices, whose communication behaviour is mostly defined in the design phase. CR devices, built on adaptable radio or SDR, might transmit in a wide range of frequencies or might change their emissions parameters given on the local spectrum environment. The capability of changing significantly the communication parameters and behaviour of SDR/CR equipment after the deployment in the market poses new problems for their validation and certification. Most of the validation and certification procedures for wireless communication equipment is based on the assumption that its behaviour is defined in the design phase.

As a consequence, it is important to define and implement innovative testing and validation techniques, which lead to an efficient and safe market deployment of new wireless communication equipment based on SDR and CR technologies. The objectives of the validation and certification phase are still the same: ensure that a product, service, or system (or portion or set thereof) continues to meet its initial design requirements, specifications, and comply with the national regulations. For example, CR devices should not generate harmful interference to primary users and be conformant to local spectrum regulations.

This report identifies the main challenges for validation and testing of equipment based on SDR/CR technologies, the main research activities in this area and the procedures and tools already defined by the industry and research community. In addition, the report also identifies mitigation techniques, which can be applied to equipment based on SDR/CR technologies after the validation and certification phase and market deployment. These mitigation techniques have the objective to minimize the impact of internal failure of the SDR/CR devices or security threats, which can be implemented by malicious attackers.

1. Introduction

Demand for services which are dependent upon access to the radio spectrum is rapidly increasing, and certain parts of the radio spectrum are becoming more and more congested. In addition, innovation is driving the development of radio technologies, which are increasingly using more sophisticated mitigation techniques in order to be able to share spectrum in various different ways amongst themselves and/or with other spectrum users.

On the other side of the coin, the European regulatory environment is evaluating how to facilitate the introduction of such innovative technologies and sharing solutions in a way that derives the maximum benefits from the usage of the spectrum. The definition of standards and regulations ensuring sufficient protection of spectrum and the citizen, while still maintaining room for innovation, is therefore becoming more and more challenging. Once technology is mature enough and, in the best case, supported by a standard, there may be a new risk or waste of resources because the implementation of the technology into interoperable products has not been carefully addressed and planned.

As a consequence, it is important to define and implement innovative testing and validation techniques, which lead to an efficient and safe market deployment of new wireless communication technologies. A range of new challenges in the validation and certification of Software Defined Radio (SDR) and Cognitive Radio (CR) persist in comparison with conventional communication systems. Despite such challenges, such verification and certification must nevertheless succeed in ensuring that a product, service, or system (or portion or set thereof) continues to meet its initial design requirements, specifications, and comply with the national regulations.

Expanding on the challenges, SDRs for example might download and activate new software modules and waveforms, posing new challenges to the certification process because their communication behaviour and parameters might therefore change after market deployment. Such technologies would have to be implemented in a way that doesn't cause interference to other systems; moreover, a range of potential challenges such as the possibility to hack SDRs and their associated radio behaviour must be guarded against. In a similar way, CR devices, built on adaptable radio or SDR, might transmit in a wide range of frequencies or might change their other emissions parameters given on the local spectrum environment, making such changes based on information obtained through an exchange with a geolocation database or perhaps spectrum sensing. Such devices must also not misbehave or fail to satisfy regulations, and their underlying processes such as information retrieval from databases and sensing schemes must remain reliable and secure.

As is clear from such examples as above, flexibility may require new validation, testing and certification procedures. In the case of SDR this might require validation and certification of the procedures and sources for radio-software, and protection mechanisms against hacking such adaptive radios, and in the case of CR it might require validation and certification of the reliability and security of geolocation database exchanges or sensing implementations. Moreover, it is noted that because CR devices might increase the risk of harmful interference to existing wireless infrastructures and communication devices, it is necessary to also consider interference mitigation techniques which can be used in post-market deployment.

In the light of the above observations, this Deliverable aims to assist the better understanding of the certification and validation challenges affecting SDR and CR.

Specifically, section 2 of this report describes current activities on validation and certification of SDR and CR technologies. Section 3 identifies the main validation and certification challenges. Section 4 describes the existing or planned validation/certification methodologies and tools defined by various entities around the world. Section 5 describes the potential mitigation techniques, which can be applied to enforce conformance to regulations after deployment of the wireless equipment based on SDR/CR. Finally, section 6 concludes the report.

2. Current activities on validation and certification of Software Defined Radio and Cognitive Radio

Demand for services which are dependent upon access to the radio spectrum is rapidly increasing and certain parts of the radio spectrum are becoming more and more congested. In addition, innovation is driving the development of radio technologies which are increasingly using more sophisticated mitigation techniques in order to be able to share spectrum in various different ways amongst themselves and/or with other spectrum users.

On the other side of the coin, the European regulatory environment is evaluating how to facilitate the introduction of such innovative technologies and sharing solutions in a way that derives the maximum benefits from the usage of the spectrum.

Various projects have investigated new procedures for validation and certification of SDR and CR equipment or they have designed and implemented test beds. The authors of this report have identified a significant divergence between two different objectives of test beds: a) the research community is more interested to define and design cognitive radio test beds to assess CR equipment from the performance/optmization point of view or to test new algorithms, b) the objective of the government/industry community is to use the test bed and field trials to assess the impact on existing radio services or to ensure the conformance of the CR equipment to regulations. While the two objectives may overlap in some cases, there is the risk that significant research efforts are not utilized efficiently.

The objective of this section is to identify and describe the current activities on validation and certification of SDR and CR technologies.

2.1 Global context

The International Telecommunication Union (ITU) an agency of the United Nations which specialises in information and communication technologies. ITU-R is the "sector" of the ITU that handles radiocommunications. One notable output of the ITU-R is a report on SDR published by its Study Group 8 (SG8) [18], which provides basic information on SDR technology and presents the application of SDR to IMT-2000 (International Mobile Telecommunication-2000) and to other land mobile systems.

In the recent World Radiocommunication Conference 2012 (WRC-2012), the action item AI 1.19 was created to consider regulatory measures and their relevance, in order to enable the introduction of software-defined radio and cognitive radio systems, in conformance with Resolution COM6/18 from the previous WRC-2007. No specific tasks are defined for the definition of test plan or validation/certification activities.

The standardization committee P1900.3 had the objective of defining recommended practices for conformance evaluations of Software Defined Radio (SDR) software modules and standards for assessing the spectrum access behavior of radio systems employing Dynamic Spectrum Access (DSA) methods. Due to lack of volunteers the committee was dismantled in 2008. A report on the activity of the committee is provided in [17].

2.2 European context

In Europe, the advisory and regulatory committee known as the Telecommunications Conformity Assessment and Market Surveillance Committee (TCAM) assists the European

Commission in conformity assessment and market surveillance matter. This committee was constituted by articles 13-15 of the Radio equipment and Telecommunications Terminal Equipment (R&TTE) directive (1999/5/EC).

Given its objectives, TCAM is involved in the revision of the R&TTE directive in order to include reconfigurable devices which might change their transmission and reception characteristics after deployment.

The revision of the R&TTE directive is still progressing, but it going to be finalized at the end of 2012. One of the main issues to be resolved is the sharing of responsibilities among the main stakeholders: hardware manufacturers, telecom operators and software waveforms producers.

2.3 European projects on validation and testing of SDR and CR

This section provides some detail on the efforts within European projects towards validation and testing of wireless equipment based on SDR/CR technologies.

2.3.1 FP7 CREW project

The “Cognitive Radio Experimentation World” (CREW) project has the objective to establish an “open federated test platform” which allows experimentally-driven research on advanced spectrum sensing, cognitive radio and cognitive networking strategies to be done by remote experimenters. The test-beds and procedures defined in the project might investigate, for example, horizontal and vertical spectrum sharing techniques in licensed and unlicensed bands.

One document produced by CREW of relevance to this report is Deliverable 4.1, which provides a definition of the test bed and scenarios. That Deliverable describes the various test scenarios considered in CREW and gives the benchmarks for each usage scenario. Such benchmarks are needed to compare results from different experiments.

The following test scenarios are identified:

- Radio environment sensing for spectrum sharing
- Horizontal sharing between heterogeneous networks in ISM bands
- Cooperation in heterogeneous networks in licensed bands
- Cognitive sensor networks
- Cognitive networks in next generation cellular systems

2.3.2 FP7 COGEU project

The “COGnitive radio systems for efficient sharing of TV white spaces in EUropean context” (COGEU) project has the objective of developing CR systems which can exploit white spaces in digital TV bands.

Technically, the mail goals are to:

- Design and demonstrate cognitive radio technologies to support mobile applications over TV white spaces (TVWS) for spectrum sharing business models.
- Quantify the impact of TVWS devices on digital TV receivers and define methodologies for TVWS equipment certifications and compliance in the European regulatory context.

COGEU will also define new methodologies for TVWS equipment certification and compliance, addressing coexistence with the DVB-T/H European standard. An important output of relevance this report is COGEU's Deliverable D4.3, which provides a description of the test-bed for coexistence evaluation. In particular, it describes the test set-ups, the wanted signals and the interference signals that are used for the measurements in the process of coexistence evaluation between DVB-T and White Spaces Devices.

The two main objectives of the test are to:

- Evaluate the interference caused by White Space devices, impacting the DVB-T receivers,
- Evaluate the performance (e.g., throughput, quality of service) of White Space devices.

2.3.3 FP7 QUASAR project (Quantitative Assessment of Secondary Spectrum Access)

QUASAR is a FP7 targeted research project (STREP) that has the objective to bridge the gap between the claims made in traditional cognitive radio research and practical implementation. The QUASAR project conducted measurements campaigns and they assessed and compared the performance of various sensing scheme and algorithm to identify the available "White Spaces" channels.

QUASAR project was mostly focused on CR test beds to validate the spectrum sensing function or to assess the availability of "white spaces".

The following deliverables are identified for their relevance to this report:

- Deliverable D2.2 Methodology for assessing secondary spectrum usage opportunities – final report. This deliverable defines the methodology to assess the availability of white spaces. It defines the methodology and tools to defined and compute the metrics and spectrum opportunities. The outlined algorithm has knowledge of primary and secondary system parameters, users' locations, and attenuations in the spectrum environment.
- Deliverable 5.4 Final Report on Models with Validation Results, which summarizes and extends the quantitative assessment of secondary spectrum opportunities for various European countries. The deliverable is based on the assessment methodology defined in QUASAR and it provides tangible conclusions on the feasibility to deploy secondary systems in Europe.

2.3.4 FP7 E3 project

The End-to-End Efficiency (E3) project was an ambitious FP7 EC Large Scale Integrated Project (IP) aiming to integrate cognitive wireless systems in the Beyond 3G (B3G) technologies. The key objectives of the E3 project was to design, develop, prototype and showcase solutions to guarantee interoperability, flexibility and scalability between existing legacy and future wireless systems.

Cognitive radio technologies are an important part of the E3 project and they are used to optimise the use of the radio resources and radio frequency spectrum on the basis of techniques like autonomic management, adaptive learning and policy management.

One document from E3 project that is of relevance to this report is Deliverable D6.4, which includes the results obtained from the validation of the E3 cognitive systems. The test challenges and techniques used in E3 are further discussed in Section 3.2.

2.3.5 FP6 WINTSEC

The WINTSEC (Wireless INTeroperability for SECurity) project had the objective to explore a mix of complementary solutions to overcome the barriers for wireless interoperability across different civil security agencies, taking into account the constraints of the security services and legacy systems and equipment. WINTSEC studies the deployment of standardized Internetworking layer at Core Network level and Software Defined Radio (SDR) technology added value for Base Stations and Terminals.

WINTSEC also addresses information assurance and security aspects.

WINTSEC project investigated the establishment of an European “SDR Certification environment”. This environment had the objective of certifying SDR Platforms and SDR Waveforms against the European “SDR Architectural Framework”, taking into account the various national constraints.

Even if the WINTSEC project was related to the civil security domain, which has different business objectives from the commercial domain, many procedures and tools can be tailored to other contexts and domains.

A description of the SDR certification activity in WINTSEC is also provided in [22].

2.3.6 FP7 EULER

The FP7 project EULER is the follower if the WINTSEC project and it has investigated the application of Software Defined Radio and Cognitive Radio techniques for Public Safety.

Project EULER designed and developed an High Data Rate (HDR) waveform to create a backbone network for SDR nodes, which are able to communicate with various communication technologies like TETRA and Satellite Communications.

Project EULER has also investigated validation and certification challenges for SDR devices in WP4. A first set of activities consists in proposing an overall approach for compliance of the SDR platform to standards. In this regard, categories and types of procedures for evaluation of ESRA compliance will be identified, and a set of well chosen and relevant procedures defined and prototyped.

In a similar way to the WINTSEC project, validation and certification procedures and tools can be tailored to the commercial domain.

2.4 European projects on validation and testing of SDR and CR

The testing and validation of CR technologies and devices in the single European member states is still limited as for In UK, in 2011, Cambridge TV White Spaces Consortium has conducted trials to evaluate and demonstrate the potential of CR technology to transmit in the Digital TV White Spaces. The consortium has evaluated CR technology against a range of applications and in various contexts: rural wireless broadband, urban dense population coverage and the emerging "machine-to-machine" communication. The result of the trials is very successful and it was found that TV white spaces can be successfully utilised to help satisfy the rapidly accelerating demand for wireless connectivity.

A description of the test plan and the related results is available at [21]. The test bed network in the trial consisted of eight base stations, deployed across urban and rural locations. The test and measurement programme included prediction of the coverage provided by the test bed base stations, which have been validated by field measurements.

The discussion on the identified testing challenges from this trail will be presented in chapter 3.

2.5 North America

The objective of this section is to provide an overview on the validation and certification procedures defined in North America (USA and Canada) in various domains: military, commercial and civil security domains.

2.5.1 USA

2.5.1.1 Commercial domain

In USA, the Federal Communications Commission (FCC) has adopted rule changes to address the certification of SDR equipment in [1], where SDR is considered a new class of equipment with streamlined equipment authorization. The purpose of the action is to modify certification rules to accommodate the flexibility offered by SDR. Specifically, FCC amended the equipment authorization rules to permit equipment manufacturers to make changes in the frequency, power and modulation parameters without the need to file a new equipment authorization application with the Commission. The action also permitted electronic labelling so that a third party may modify a radio's technical parameters without having to return it to the manufacturer for re-labelling current commercial waveforms [13].

2.5.1.2 Civil Security and Military domains

2.5.1.2.1 Joint Tactical Radio Systems (JTRS) Technology Laboratory (JTel)

In US, the JTRS Technology Laboratory (JTel) is the testing and certification arm of the JTRS JPO for software defined radio technologies.

JTel has various responsibilities, which include:

- the definition of a JTR set operative environment, which is compliant to SCA
- the definition of a test bed and test procedures for the certification of SCA-compliant SDR in the military domain.
- maintain a repository of all the certified JTRS waveforms and related tools and products.

2.5.1.2.2 DARPA XG

The Defence Advanced Research Projects Agency (DARPA) has financed the Next Generation (XG) programme to develop system concepts and technologies to enhance military communications through Dynamic Spectrum Access (DSA) and Cognitive Radio (CR).

One of the stated objectives of the XG program is to demonstrate that cognitive radio can produce at least the performance of a conventional radio but accomplish this with improved efficiency through adaptation of transmission parameters on the basis of the information received from the environment. A detailed description of the DARPA XG program is out of the scope of this report and is provided in [30].

Validation and testing activities have been carried out and they are described in various references. In [31], fields test were executed to validate the policy management systems of the XG radios. Four test scenarios were executed: a) No use of the Policy Management, b) Limited Policy Operation, c) Enhanced Signal-based Policy and d) Enhanced Location-based Policy. Various performance metrics were used. They included the a) spectrum evacuation time to avoid transmitting in spectrum bands occupied by the primary users, b) the scalability of the policy framework with the increase of number of policies or devices, c) the effectiveness of the policy reasoning engine to execute the correct behaviour and d) the level of interference generated to the primary users.

2.5.1.2.3 DARPA WNAN

The DARPA Wireless Network After Next (WNAN) programme is working on the development of affordable handled communications for the “individual warfighter”, leveraging inexpensive commercial parts. A key aspect of the handheld communications devices will be dynamic spectrum access capability. In that sense, WNAN takes into account the wealth of knowledge obtained in the XG program, aiming to support the opportunistic usage of locally available spectrum by army personnel in area of the world in which it might not be easy to access spectrum for such usages.

2.5.2 Canada

The Communication Research Centre (CRC) of Canada has developed a Wi-Fi based CR networking system called CORAL [51], to prototype, test and evaluate various concepts of CR technology. The CORAL system was designed as a research network, which links universities and research in a live Wi-Fi network.

CORAL uses the ISM unlicensed bands at 2.4 and 5.8 GHz and is currently a fixed network, even if there are plans for a future mobile development [51].

CRC has defined API and has developed various tools to support the deployment of the Wireless Fidelity (WiFi) CR testbed. In particular the Radio Environment Awareness Map (REAM), which is a core element of CORAL. An overview of the CORAL system is provided also in [52].

Even if CORAL is a complete package with a remarkable level of maturity, the effort towards validation and testing procedures and tools is still limited as this was not the main objective of the CORAL project.

2.6 Asian context

The objective of this section is to provide an overview on the validation and certification activities for SDR and CR technology in Asia.

2.6.1 Japan

On 2008, In Yokosuka Research Park in Yokosuka City, the Japanese NICT research center has deployed several kinds of test beds of cognitive radio. In carrying out field tests, evaluations and demonstrations of cognitive radio, NICT carried out several field experiments using these test-beds from the early stage of cognitive radio research and developments. The CR devices used in the test bed support an extremely wide frequency band of 400 MHz-6 GHz and supports various communication systems. The test results have shown that the error vector magnitude (EVM) was lower than 3% on the sending side and lower than 11% on the receiving side. The measured dynamic range was higher than 50dB on 400MHz and 5GHz bands. The noise figure (NF) on the sending side was lower than 5dB on 400MHz and 2GHz bands, and lower than 15dB on a 5GHz band.

In April 2010, NICT started field trials of CR technology in the city of Fujisawa. The CR nodes were developed on the standard Institute of Electrical and Electronics Engineers (IEEE) 1900.4. The main server has been set at the NICT Yokosuka research Centre.

During the operation, NICT has distributed 500 CR nodes in the city of Fujisawa, which were able to provide internet access to any users who want to access the internet.

During the field trial, NICT has collected both traffic data and controlling data, which have been subsequently analyzed to verify the performance and improve the next release of cognitive radio systems. The trials and the related results are expected to contribute to draft new regulations and support the development of these technologies. There is also the idea to apply these technologies to define Mobile Virtual Network Operator (MVNO).

After this field trial, NICT has continued the research and development of cognitive radio solutions in the white spaces of television broadcasting frequency bands.

Furthermore, NICT will integrate concepts of virtual network technology into the cognitive routers.

2.6.2 Singapore

In Singapore, the Infocomm Development Authority of Singapore (IDA) is promoting “White Space Technology Trials”. The IDA recognizes the potential of “white space” concept and will conduct trials for white space technology. On 7 April 2010, IDA announced the 'White Space Technology Information Package and Test Plan' at the IEEE International Dynamic Spectrum Access Networks (DySPAN) 2010 symposium held in Singapore, where organizations were requested to indicate their interest in participating in white space trials.

The upcoming trials, named Cognitive Radio Venues ("CRAVE"), will support IDA in developing the regulatory framework for the definition of TV geo-location databases. One of the purposes of the trials is to obtain real-world measurements, which would facilitate in the development of white space devices.

The test plan used in the trial is described in [20].

There were two main categories of tests: controlled test in the laboratory and test done in the field.

In both categories, three different test plans were executed:

- TV Signals. This test plan included all the tests to validate the capability of the CR device to avoid the generation of harmful interference to TV signals. In particular, the sensing of TV signal (single or multiples) was tested, the capability to detect and avoid a TV signal and the level of interference of CR device to TV signals.
- Wireless Microphone Signals. This test plan included all the tests to validate the capability of the CR device to avoid the generation of harmful interference to

Wireless Microphone signals. In particular, the capacity of detecting the wireless microphone signals and the generation of interference to them.

- Operational environment (only in the controlled category). This test plan was focused on a CR capability of sensing TV signals and avoiding them with different values of the power of the TV signals.

The entire set of tests was executed successfully.

3. Validation and Certification challenges

This section describes the main validation and certification challenges for SDR and CR technology in comparison to conventional communication technologies.

3.1 Background research

This section provides a survey of the current state of art on validation and certification challenges from journals/conference papers.

The research activity on this area is quite limited.

Reference [17] describes the activity of P1900.3 and identifies the following categories for testing:

- Over The Air (OTA) Provisioning Testing – Verifies the ability of a device to correctly obtain and install applications over the air and to communicate problem with a provisioning server.
- Security Testing – Verifies sandbox boundaries and privileges of midlets plus verifies Mobile Information Device Profile (MIDP) 2.0 security model.
- Performance Testing – Measures the time required for a device to perform operations or combinations of operations.
- Stress Testing – Tests the behaviour and robustness of the implementation when stretched to the limits of system resources. Ensures that device does not crash during continuous execution.

Reference [17] acknowledges the presence of significant challenges to certify SDR devices. The main challenge is the presence of non-functional attributes, where the cause-effect behaviour cannot readily be specified. Complex systems commonly exhibit such non-functional attributes due to the exceedingly large potential state space. SDR is considered a complex system because of the large potential state space of different combinations of hardware platforms and waveforms and the range of frequency where SDR can operate.

Reference [23] provides a description of the certification process for SDR devices developed upon the Software Communications Architecture (SCA). No significant challenges are described but critical areas of certification are identified.

Reference [10] describes the Iris test-bed for cognitive radio devices. Various challenges are identified in the paper:

- Testing repeatability was not easy to achieve.
- Benchmarks for cognitive radio networks are not clearly defined yet.
- There is not enough attention from the academic community to validation and testing of cognitive radio networks.
- Standards are not fully completed. As a consequence, it is difficult to define complete test procedures.

Reference [14] describes the Cogito test bed for Cognitive radio networks. One significant challenge was that some tests were not repeatable. Propagation and communication uncertainty prevented the repetition of test results.

Reference [32] describes a measurement test bed to measure the Minimum Response Delays of real CR devices, which is usually not addressed in the theoretical framework. The paper used the measurements to guide the implementation work and to verify algorithm performance.

Reference [33] describes a cognitive radio test-bed for physical and link layer experiments. The main objective of the paper is to demonstrate that practical implementation of cognitive radio networks are able to implement spectrum-sensing to identify the presence of Primary Users (PU) and avoid creating harmful interference. The paper identifies various testing parameters, which include:

1) The time until detection of the Primary User.
2) The reliability of Primary User detection.
    a) The probability of not detecting the Primary User (false negative).
    b) The probability of false alarms (false positive).
3) The time needed to clear the spectrum once a Primary User has been detected.

Reference [34] describes a real time test-bed for the evaluation of the cognitive radio Medium Access Control (MAC) algorithm. The authors of the paper implemented a cognitive radio MAC algorithm based on the SoC programmable processors. The performance of the implementation was evaluated on the basis of parameters like collision probability, traffic capacity and conformance to the time thresholds.

Reference [35] describes the testing and evaluation of Policy-driven Dynamic Spectrum Access (DSA) radios. The approach of the paper is to augment existing standards for testing and evaluation of wireless communication systems to address the performance of specific DSA features. The framework proposed by the authors addresses both radio frequency (RF) aspects of DSA as well as the overall network performance of DSA systems.

The paper describes various metrics to evaluate the performance of the DSA network. This list includes (it is not an exhaustive list of the parameters specified in the paper):

- Abandonment time, which characterizes the time required for the DSA network to abandon a channel assigned to a spectrum user.
- Base Network Migration time, which characterizes the time it takes for the Policy based master node in the DSA network to find an occupied frequency and start transmitting.
- Network Reconnect time, which is the time for a DSA node to reconnect to the network and to be operational.
- Migration time, which is the time for a DSA networks to reconfigure itself after that the DSA master node has decided to leave a frequency band, because it is generating harmful interference to a primary user.
- Power Control time, which is the time for the DSA node to readjust their transmission power level to mitigate wireless interference.

Reference [34] also introduces the concept of defining testing scenarios, which can reproduce a particular scenario. The paper identifies the following key scenarios:

a) Urban Environment, which is characterized by building obstructions, indoors and outdoors communications, and very dense RF spectrum utilization.

b) Clear Line of Sight, which is characterized by unobstructed, level terrain (or naval or aerial environment), where line of sight is always maintained.

c) Unlevel Terrain, which is characterized by the presence of natural obstacles like hills and mountains or different environment conditions, which can affect radio propagation like various salinity and sea state conditions.

These scenarios have been defined with military applications in mind, but they could be also adapted to commercial applications.

3.2 Identification of the challenges

This section identifies the main challenges for testing and validation of Software Defined Radio and Cognitive Radio technology.

3.2.1 Generic Challenges

- A significant challenge for the definition of a realistic test bed is scalability. Existing Cognitive radio networks test bed are usually small (just few radio nodes) and based on the same platforms. These test beds do not address issues of scalability of aggregated interferences, which will definitively occur in real-world future cognitive radio deployments.
- As described before, a significant challenge is the large state space of combinations of hardware platforms and waveforms for SDR and range of frequencies/transmission parameters for CR devices. Alternatively, because of the high flexibility of SDRs it is not always easy to ascertain the boundaries of their capabilities that should be tested.
- Because of the high degree of reconfigurability of CR devices, a significant challenge is to development and testing of a user-modifiable protocol stack that can run on the devices (see [26]).
- As described in [27], wireless network simulation tools, which are designed for conventional wireless communication systems are mainly focused on layer-2 and layer-3 of the communication stack. CR networks are usually based on the knowledge of the physical layer (e.g., spectrum sensing) and it is critical to incorporate faithful physical models into these tools.
- In comparison with conventional wireless communication devices, SDR technology does not specify one common processing platform. Tools and procedures already defined for specific hardware platforms should be modified for SDR technology. This problem is obviously more important in “white box” testing in comparison with “black box” testing.

3.2.2 Challenges for specific cognitive radio use cases and technologies

3.2.2.1 Dynamic Spectrum Access

- In comparison to conventional wireless networks, DSA networks can change the spectrum allocation and usage in time, space and frequency (i.e., DSA dimensions).

Most of the network engineering tools are designed to optimize the static allocation of spectrum bands over the territory. It may be difficult for network operators and the related validation and testing teams to ensure that the coverage of the DSA networks will be conformant to spectrum regulations and that no harmful interference will be created in any point of the DSA dimensions.

- The reallocation of spectrum bands among different DSA networks will be based on the coordination of the respective DSA network operators. This is a new paradigm, which will require new testing and certification procedures.
- Laboratory testing is a practical and efficient way to test the metrics and the features of DSA nodes and the overall DSA network, but field test is necessary to ensure the correct behaviour of the DSA network in the field. For example, the hidden node problem may not be tested correctly in a lab environment. The challenge is to identify realistic field testing scenarios, which can evaluate the performance of DSA networks. As described in [34], more than one operational scenario should be defined.
- The design of DSA networks could be based on cognitive control channels (CCC), which are used to distribute the information on the potential spectrum bands and the need to reallocate the channels. Validation and testing of the CCC is very important to evaluate the resilience of the overall DSA network. The CCC may interface many different networks. A potential challenge is to define exhaustive testing procedures to verify all the potential interfaces of the CCC.

3.2.2.2 *Opportunistic/secondary spectrum access*

The following validation and testing challenges are identified for secondary access:

- Low Power Level for detection: In a similar way to Detect and Avoid (DAA) UWB devices, CR devices must detect very low power levels of the incumbent signal (e.g. -100-130 dBm per MHz as indicated in [28]). Measurements at these low power levels can be quite challenging for a test-bed.
- Timing: Manual test methods make timing-related measurements inaccurate. As an example, the analyzers are required to start capturing the signal at the same instant the device is powered on, which is a hard task when using manual test methods. This challenge is important in the validation of detect and avoid of transmission in the "White Spaces" bands by CR devices.

In this technical report, UltraWideBand is considered a particular case of secondary access.

Validation and testing of UWB has also its own specific challenges as described in [24]:

- Low Power Level: Due to the low power levels to be detected, as well as the power levels to be measured (-80 dBm/MHz in Zone 1) when in Non-Interference Mode (NIM), a dynamic margin problem can arise, as these levels are close to the noise floor limit of most conventional spectrum analyzers (-70 dBm/MHz). This constraint is much worse in radiated test environments. Furthermore, the low power UWB signal must be detected and discriminated in the presence of the victim signal. As a consequence, test equipment must have high sensitivity to precisely detect the uplink victim signal as defined by regulators.

- Realistic scenarios: The behavior of the victim service device and the UWB device should be recreated in the testing environment.
- Timing: Manual test methods make timing-related measurements inaccurate. As an example, the analyzers are required to start capturing the signal at the same instant the device is powered on, which is a hard task when using manual test methods.
- Detection Probability. Generally it takes considerable time to measure the detection probability because it is calculated as an average on a large number of measurements. It is important to define alternate methods, which still validate the testing requirement but reduces the testing time.
- Radiated tests: In radiated test environments, problems can arise when measuring power levels, specifically interfering levels and power levels transmitted by the DUT (Device Under Test), since the positions of the test and interfering antennas relative to the DUT position are different. The radiation pattern of the DUT's receiving antenna might not be symmetrical in azimuth, and thus the DUT needs to be rotated in order to search for the maximum receive and transmit power levels, which can be at different positions.

3.2.2.3 Collective Use of Spectrum (CUS) – Unlicensed

The following validation and testing challenges are identified for collective use of spectrum:

- In comparison to other spectrum models, CUS networks can be based on various dimensions to improve spectrum utilization in an area. These "dimensions" can be time, frequency, space as in the other spectrum models but also coding, packet contention, directional spacing (e.g., MIMO technique). A potential challenge is to define test procedures, which addresses all these dimensions in a complete and exhaustive way.
- As described in the general challenges, scalability could be an important challenge for the testing and validation of Cognitive Radio Networks. This challenge is even more relevant for CUS spectrum model, where the same frequency bands can be used by many radio devices in the same area.

3.2.3 Software Defined Radio

As described in section 3.1 and reference [17], a significant challenge for SDR validation and testing is the very large state model of the potential combinations of hardware platforms and software waveforms. Another potential challenges is the lack of maturity and completeness of the standards, including even de-facto standards like the Software Communication Architecture (SCA) [53].

Even with these challenges, the experience on SDR certification is more mature than CR technology as shown by various references like [23], which identifies and describes key procedures for SDR evaluation and certification.

4. Validation/certification methodologies and tools

This section provides a survey of the existing methodologies and tools for testing software defined radio and cognitive radio.

4.1 Introduction

Cognitive radio technology will require new methodologies and tools or an evolution of existing ones. As described in section 3, the new testing and certification challenges will be present. The reconfigurability, dynamicity and flexibility of CR technologies would probably require tools, which are able to test the behaviour of the equipment not only for static design but also for the dynamic behaviour.

In a similar way, the reconfigurability of Software Defined Radio may require new tools for testing the various combinations of HW platforms and SW waveforms.

4.2 Methodologies

No standards testing methodologies have been defined for Cognitive Radio. Existing testing methodologies could be extended to cognitive radio networks. For example, Capability Maturity Model Integration (CMMI) testing methodology described at http://www.sei.cmu.edu/cmmi/.

A specific methodology for Cognitive Radio technology is proposed in [27]. The methodology is called REM-based radio scenario-driven testing (REM-SDT). The CR network under test is subjected to various realistic situations stored in the Radio Environment Map (REM), which could be in form of machine-readable Extensible Markup Language (XML) files. The REM scenarios are coupled with Monte Carlo simulations to create different combinations of test scenarios.

4.3 Tools

The objective of this section is to describe tools, which can be used for the validation and certification of wireless equipment based on SDR and CR technologies.

4.3.1 Software Defined Radio

Currently JTRS Test Application (JTAP) is the only known SCA 2.2.2 test tool for certification of the operating environment and the waveform. However, it is not released by JTRS yet.

Joint Program Executive Office (JPEO) and JTRS Test and Evaluation Laboratory (JTEL) does have other software test tools called the Waveform Test Tool WTT and the Data Reduction Parser (DRP). However, both software applications apply and test SCA requirements for version 2.2 only.

JTAP allows for the inclusion of custom implementation of test cases by test developer.

4.3.2 Cognitive Radio

Currently, there are no standard tools for testing and validation of Cognitive Radio networks. Tools already defined for testing wireless communication technologies, can be extended to test cognitive radio technologies [36].

One example is the Testing and Test Control Notation Version 3 (TTCN-3) described at http://www.ttcn-3.org/.

TTCN has already various commercial tools, which can support the testing and validation process. The list of available TTCN tools is identified at http://www.ttcn-3.org/CommercialTools.htm.

5. Mitigation techniques to enforce conformance to regulations after deployment

The purpose of this section is to identify and describe potential mitigation techniques to be adopted after the market deployment of wireless communication system based on SDR/CR technologies.

5.1 Introduction

Even after the validation and certification phases, SDR and CR equipment could malfunction or be subject to security threats like any other computing device.

The purpose of this section is to describe potential mitigation or protection techniques, which could be used to improve the robustness of SDR and CR equipment against security threats or internal malfunction.

A survey of security threats and related mitigation techniques for CR networks is presented in [37]. The list of security threats includes not only external attacks from malicious parties but also malfunctions due to internal failure or due to lack of knowledge of the environment like in the Hidden Node problem.

A complete list of the potential security threats to SDR and CR is out of the scope of this technical report.

Only the most significant threats are identified:

1. Malicious alteration of CR equipment. For example, a CR node or network can be taken over by another party to release spectral bands, which can be used by the malicious attacker.
2. Denial of service attack to functions of the CR Network. For example, jamming of the cognitive control channel.
3. Unauthorized use of bands by an external party.
4. Internal malfunction of the CR equipment.
5. Download and activation of malicious software (i.e. waveform) on the SDR platform.
6. Hidden node problem.

The impact of these security threats can vary. In comparison to conventional wireless communication network, a significant impact is the capability of jamming or creating interference to primary users because CR devices can theoretically transmit in a range of frequencies, which is not defined in the design phase of the equipment. Another impact is the disruption of the CR network itself.

Finally, another potential issue is the impact of aggregated interference of secondary devices against primary devices. Spectrum masks defined by regulators and certification procedures could be appropriated against typical operational scenarios, which have well defined upper limits for the density of CR devices in an area. In some cases like a major event (e.g., concert, sport event) the density of CR devices may be higher than expected. It is important to identify mechanisms to mitigate the risk of elevated aggregated interference from high density CR networks.

The next section will identify the potential mitigation techniques, which can be implemented to address these threats and issues.

5.2 Mitigation techniques

5.2.1 Mitigation techniques for software radio equipment

Digital signatures can be used to protect SDR equipment from the download and activation of malicious software like a corrupted waveform. The application of digital signatures to SDR technology is described in [38], where the proposed security framework is based on public/private key scheme for the authentication and verification of software, which can be downloaded and activate on the SDR platform. As described in [38], the manufacturer generates a digital signature of the software waveform after certification, which is usually implemented as a hash and an encryption function. The digital signature is then added to the software file of the waveform. The software file is then encrypted with a secret key, which is unique to each terminal. The secret key is stored in tamperproof hardware on the terminal device. Since symmetric encryption techniques are used, encryption and decryption is fast. The software waveform file is then released for deployment in the network. A potential limitation of this technique or similar techniques based on digital signatures is scalability.

Trusted Computing (TC) has been also proposed to ensure that only authorized software is executed on the SDR platform. The application of TC to SDR technology is described in [39].

5.2.2 Mitigation techniques for cognitive radio equipment

Reputation mechanisms can be implemented to protect a CR network from attackers or malfunction of the CR nodes as described in reference [40]. For example, in the spectrum sensing function, a CR node can be classified at different levels of reputation or trust on the basis of spectrum sensing information, which they provide to the other nodes in the CR network. If the information is not correct after a number of iterations, then the contribution of that specific CR node is considered not valid, which may hint to a security threat or the presence of a malicious CR node.

Even if other mitigation techniques may fail, it is still possible to implement a protection mechanism in the SDR/CR node to ensure that it can only transmit in the spectrum bands allowed by the spectrum regulators. This mechanism is called Automatic Calibration & certification Unit (ACU) in reference [41]. The ACU is responsible for controlling the output spectrum to be compliant to the radio regulation parameters. The ACU stores the local constraints on spectrum emissions in configuration files. On the basis of its location (e.g., provided by GPS), the ACU verifies that the transmission requests by the SDR/CR functions are compliant to the configuration files. Even if the CR node is malfunctioning or it has received wrong information from other nodes, it is not allowed to transmit by the ACU.

Even if the CR device has implemented ACU and other security protection techniques to protect itself against malicious attackers, it can still generate harmful interference to primary users in the area if its knowledge of the spectrum environment is incorrect. One potential scenario of this context is called "Hidden Node problem".

The Hidden Node problem is a known problem in wireless communication systems and not only in cognitive radio technology. The Hidden node problem and related mitigation techniques have been described in [42] for Wi-Fi networks and for Wireless Personal area networks (WPAN) based on IEEE 802.15.4 in [43]. For these technologies, the issue is the lack of knowledge on the presence of terminals in the area and the lack of synchronization among terminals.

In the case of CR networks, the Hidden node problem is mostly related to failures of the spectrum sensing function. In this case, a CR node has an uncorrected estimate of the emission power of the primary users because of the presence of natural or man-made obstacles (e.g., hill or building), which create shadowing effects. Because of the presence of an obstacle, the spectrum sensing function of the CR device may detect low power levels of the primary user, which may indicate an incorrect location of the primary user base station. Due to the uncorrected estimate, the CR device may reach the false conclusion that it can transmit its own signal at a high power because of the absence of primary users in the area. By transmitting at high power, the CR device can generate harmful interference to primary user receivers (e.g., Digital TV - DTV receivers), which are not shadowed by the obstacle.

Various mitigation techniques have been proposed in literature to mitigate the impact of the “Hidden node problem”. A common approach is to improve the knowledge of the radio frequency spectrum environment through a cooperative or collaborative approach at the level of the CR network. Collaborative spectrum sensing has been proposed in various references including [46], which discusses the benefits gained by cooperative spectrum sensing to overcome the limitations of individual spectrum sensing challenges such as hidden terminal problem, shadowing, fading, and hardware limitations. The study provides a review of cooperative spectrum sensing techniques along with the various sensing schemes that implement these techniques. The paper shows that cooperative spectrum sensing can improve the cognitive radio network performance by increasing spectrum efficiency and providing a better detection accuracy. However, the benefits come at the cost of increased overhead traffic, power consumption, complexity, and the need for control channels.

The spectrum sensing function could be also separated from the other functions in the CR networks. References [44] and [45] propose a network structure where the spectrum sensing task is separated from the unlicensed users (secondary users). The service provider for the secondary users needs to place sensing devices within the networks of licensed users (primary users). These sensing devices sense the primary users’ activity. This approach is convenient also from a business model point of view because the sensing function is implemented in devices provided and deployed by the CR network provider instead of low cost consumer products. The disadvantage is that the coverage of the sensing devices may not be extensive as the area used by the secondary devices and the deployment of such network can be quite expensive. This function is also called spectrum monitoring.

An alternative approach is presented in [47], where is presented an Integral Equation based propagation method, which can be used in conjunction with a Radio Environment Mapping (REM) server to address the ‘Hidden Node Problem’ in Cognitive Radio (CR) technology. The idea is to create and update a REM, which is initially based on signal strength predictions and the known position of the primary users. The spectrum readings from CR devices or monitoring stations can be used to improve the knowledge of the REM and detect “gaps” or anomalies, which can identify the presence of hidden node problems in the area.

To address the issue of aggregated interference in high density CR networks, various techniques have been proposed: lower the emissions of CR devices, mitigate the effect of aggregated interference or implement an administrative management systems to shutdown or change the transmission parameters of CR devices.

Reference [48], deals with the problem of aggregated interference generated by multiple cognitive radios (CRs) base don IEEE 802.22 at the receivers of primary (licensed) users. The CR network (CRN) is modelled as a multiagent system where the multiple agents are the different secondary base stations in charge of controlling the secondary cells. The paper proposes real-time multiagent reinforcement learning, which is known as decentralized Q-learning, to manage the aggregated interference generated by multiple CRNs. By directly interacting with the surrounding environment in a distributed fashion, the multiagent system is able to learn, in the first case, an efficient policy to solve the problem and, in the second case, a reasonably good suboptimal policy. The paper also provides simulation results, which show that the signalling overhead to control the level of aggregated interference is minimal.

Another approach is proposed by [49], where a beacon transmitter is used at the location of the PU transmitter or at the location of the PU receiver. The paper also investigates the cooperative sensing effect on the aggregate interference statistical model. The paper defines an aggregate interference model and evaluate the effect on the performance of a network with a beacon consisting of multiple SUs and a single PU is investigated. The metrics used to evaluate the performance of the model is the capacity-outage probability of the PU.

Reference [50] investigates the application of power control, contention control or hybrid power/contention control schemes to mitigate the impact of aggregated interference of secondary users (SU) to primary users (PU). The paper describes two cases: a) a power control scheme is proposed to govern the transmission power of a CR node, b) a contention control scheme at the media access control (MAC) layer is proposed to coordinate the operation of CR nodes with transmission requests. The probability density functions (PDFs) of the interference received at a primary receiver from a CR network are derived numerically for both cases. The paper also investigates and models the hybrid case, where power and contention controls are jointly adopted by a CR node. The contribution of the paper is valuable because it also investigates the case of a hidden primary receiver and it evaluates the impact of interference at the PU receiver. The paper demonstrates that both power and contention controls are effective approaches to alleviate the interference caused by secondary CR networks.

The referenced papers are relatively recent and the research activity in this field is still continuing. In many cases, standardization on mitigation techniques is still in early phase, especially for the mitigation of aggregated interference.

6. Conclusions

Validation and testing of SDR and CR equipment can be a complex activity, which is still very much in the development process. While some existing validation and testing techniques for conventional wireless communication systems can be extended to SDR/CR technology, there are specific challenges which must be addressed in the cases of SDR/CR. In particular, the capability of dynamically changing transmission parameters and the spectral bands, which would conventionally be fixed in hardware, and the capability of downloading and activating new software waveforms, must be taken into account. Means must be ingrained to make sure that the adaptations of such devices are reliable and secure, and that the range of possible configurations of such devices are test, or their bounds of operation. Because configurations and situations which were not predictable prior to deployment might arise with such devices, means for in-the-field testing must be devised.

Further studies are needed by the industry and research community to define and standardization testing procedures for SDR and CR equipment. In addition, it is also recommended to implement mitigation techniques in SDR/CR equipment to address specific security threats or malfunctions, which can negatively impact primary users through harmful wireless interference. One important example is the mitigation of aggregated interference by secondary users against primary users. A list of the potential mitigation techniques has been presented in this report.

.

7. References

[1] *Federal* Communication. Commission, “In the matter of Authorization and Use of Software Defined Radios, First Report and Order,” Sept. 2001, FCC 01-264, ET Docket No. 00-47.

[2] FCC, “Second report and order and memorandum opinion and order,” in FCC 08-260, Nov. 2008.

[3] European Radio equipment and Telecommunications Terminal Equipment (R&TTE) Directive (1999/5/EC).

[4] Franklin, A.A.; JinSuk Pak; HoiYoon Jung; SangWon Kim; SungJin You; JungSun Um; SunMin Lim; GwangZeen Ko; SungHyun Hwang; ByungJang Jeong; MyungSun Song; ChangJoo Kim; , "Cognitive Radio test-bed based on ECMA-392 International Standard," *Wireless Communication Systems (ISWCS), 2010 7th International Symposium on* , vol., no., pp.1026-1030, 19-22 Sept. 2010.

[5] Sahai, A.; Woyach, K.; Atia, G.; Saligrama, V.; , "A technical framework for light- handed regulation of cognitive radios," *Communications Magazine, IEEE* , vol.47, no.3, pp.96-102, March 2009.

[6] Mueck, M.D.; Haustein, T.; Bender, P.; , "Digital and dynamic certification in the framework of the novel revised R&TTE Directive in Europe," *Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 2011 Sixth International ICST Conference on* , vol., no., pp.166-170, 1-3 June 2011.

[7] Hanwen Cao; Konig, C.; Wilzeck, A.; Perez Guirao, M.-D.; , "Cognitive Agile Networking testbed," Radio and Wireless Symposium (RWS), 2010 IEEE , vol., no., pp.296-299, 10-14 Jan. 2010.

[8] Budihal, R.; Jamadagni, H.S.; , "Hybrid approach to Cognitive radio test bed," *Ultra Modern Telecommunications & Workshops, 2009. ICUMT '09. International Conference on* , vol., no., pp.1-7, 12-14 Oct. 2009.

[9] Nolan, K.E.; Sutton, P.D.; Doyle, L.E.; Rondeau, T.W.; Le, B.; Bostian, C.W.; , "Dynamic Spectrum Access and Coexistence Experiences Involving Two Independently Developed Cognitive Radio Testbeds," *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on* , vol., no., pp.270-275, 17-20 April 2007.

[10] Doyle, L.E.; Sutton, P.D.; Nolan, K.E.; Lotze, J.; Ozgul, B.; Rondeau, T.W.; Fahmy, S.A.; Lahlou, H.; DaSilva, L.A.; , "Experiences from the Iris Testbed in Dynamic Spectrum Access and Cognitive Radio Experimentation," *New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on* , vol., no., pp.1-8, 6-9 April 2010.

[11] Cognitive Radio Platforms and Testbeds. Cognitive Radio Communications and Networks, 2010, Pages 539-585.

[12] Proposed Certification Test Procedures for TV Band (White Space) Devices Authorized Under Subpart H of the Part 15 Rules.

[13] Wang, Y.; Simon, M.; Bonde, P.; Harris, B.; Teuteberg, J.; Kormos, R.; Antaki, J.; , "Prognosis of Right Ventricular Failure in Patients with Left Ventricular Assist Device Based on Decision Tree with SMOTE," *Information Technology in Biomedicine, IEEE Transactions on* , vol.PP, no.99, pp.1, 0.

[14] Pratas, N.; Meucci, F.; Zrno, D.; Prasad, N.R.; Rodrigues, A.; Prasad, R.; , "Cogito test-bed - wireless research evolved," *Cognitive Radio and Advanced Spectrum Management, 2009. CogART 2009. Second International Workshop on* , vol., no., pp.116-121, 18-20 May 2009.

[15] Giorgetti, A.; , "Interference mitigation technique by sequence design in UWB cognitive radio," *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on* , vol., no., pp.1-5, 7-10 Nov. 2010.

[16] Rahman, M.; Yanikomeroglu, H.; Wong, W.; , "Interference Avoidance with Dynamic Inter-Cell Coordination for Downlink LTE System," *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE* , vol., no., pp.1-6, 5-8 April 2009.

[17] J. Giacomoni and D.C. Sicker, "Difficulties in providing certification and assurance for software defined radios," *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, vol., no., pp.526-538, 8-11 Nov. 2005.

[18] ITU, "The Impact of Software Defined Radio on IMT-2000, the Future Development of IMT-2000 and Systems Beyond IMT-2000," in ITU-R Report 2063.

[19] Report on Japan Study in Cognitive Radio and Networks, Code OHTI 93/25/2010. www.tekes.fi.

[20] Trial of White Space Technology accessing VHF And UHF Bands in Singapore http://www.ida.gov.sg/doc/Policies%20and%20Regulation/Policies_and_Regulation_Level2/WST/WhiteSpaceTP.pdf

[21] Cambridge White Spaces Consortium. Cambridge TV White Spaces Trial. A Summary of the Technical Findings. 2012. Available at: http://www.cambridgewireless.co.uk/docs/Cambridge%20White%20Spaces%20Trial%20-%20technical%20findings-with%20higher%20res%20pics.pdf. Last accessed 30 June 2012.

[22] Symeonidis, D.; Baldini, G. "European Standardization and SDR Certification," *Telecommunications (AICT), 2010 Sixth Advanced International Conference on*, vol., no., pp.136-141, 9-15 May 2010.

[23] Test and Certification Guide for SDRs based on SCA. Part 1: SCA. Wireless Innovation Forum SDRF-08-P-0007-V1.0.0.

[24] Gianmarco Baldini, Detlef Fuehrer, Janie Banos, Manuel García Fuertes, Xiaochen Chen, Di Wu, Measurement and functional validation of detect and avoid ultra wideband devices, *Measurement*, Volume 45, Issue 5, June 2012, Pages 1001-1014, ISSN 0263-2241..

[25] Krah, A.; Grimm, M.; Murtaza, N.; Kotterman, W.; Landmann, M.; Heuberger, A.; Thoma, R.; Hein, M.; , "Over-the-air test strategy and testbed for cognitive radio nodes," *General Assembly and Scientific Symposium, 2011 XXXth URSI* , vol., no., pp.1-4, 13-20 Aug. 2011.

[26] K. R. Chowdhury and T. Melodia, "Platforms and testbeds for experimental evaluation of cognitive ad hoc networks," *IEEE Communications Magazine*, vol. 48, no. 9, pp. 96–104, 2010.

[27] Youping Zhao; Shiwen Mao; Neel, J.O.; Reed, J.H.; , "Performance Evaluation of Cognitive Radios: Metrics, Utility Functions, and Methodology," *Proceedings of the IEEE* , vol.97, no.4, pp.642-659, April 2009.

[28] CEPT ECC Report 159 "Technical and operational requirements for the possible operation of cognitive radio systems in the 'White spaces' of the frequency band 470-790 MHZ, Feb. 2011.

[29] Szelest, Marcin; Uzdrzychowski, Wojciech; Grzechca, Damian; , "GNU radio and USRP2 as a universal platform for verification of wireless communication devices used in automotive applications," *Mixed Design of Integrated Circuits and Systems (MIXDES), 2012 Proceedings of the 19th International Conference* , vol., no., pp.436-440, 24-26 May 2012.

[30] McHenry, M.; Steadman, K.; Leu, A.E.; Melick, E.; , "XG DSA Radio System," *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on* , vol., no., pp.1-11, 14-17 Oct. 2008.

[31] Perich, F.; Foster, R.; Tenhula, P.; McHenry, M.; , "Experimental Field Test Results on Feasibility of Declarative Spectrum Management," *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on* , vol., no., pp.1-10, 14-17 Oct. 2008.

[32] Zhe Chen; Nan Guo; Zhen Hu; Qiu, R.C.; , "Experimental Validation of Channel State Prediction Considering Delays in Practical Cognitive Radio," *Vehicular Technology, IEEE Transactions on* , vol.60, no.4, pp.1314-1325, May 2011.

[33] Mishra, S.M.; Cabric, D.; Chang, C.; Willkomm, D.; van Schewick, B.; Wolisz, S.; Brodersen, B.W.; , "A real time cognitive radio testbed for physical and link layer experiments," *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on* , vol., no., pp.562-567, 8-11 Nov. 2005.

[34] Shen Gu; Pengchao Xu; Xinbing Wang; Xiaoying Gan; Hui Yu; , "A Real Time Testbed for the Evaluation of Cognitive Radio MAC," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* , vol., no., pp.1-5, 6-10 Dec. 2010.

[35] Boksiner, J.; Kauteng Chang; Costello, P.; Huck, R.; Leising, T.; Zankel, M.; Posherstnik, Y.; Totaro, M.; Trang Mai; Molnar, J.; , "Testing of policy-based dynamic spectrum access radios," *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010* , vol., no., pp.773-778, Oct. 31 2010-Nov. 3 2010.

[36] J. Poncela, J. T. Entrambasaguas, and M. C. Aguayo-Torres. 2010. Advancing Radio Testing Methodology via Formal Notations. *Wirel. Pers. Commun*. 53, 3 (May 2010), 409-429.

[37] Baldini, G.; Sturman, T.; Biswas, A.R.; Leschhorn, R.; Godor, G.; Street, M.; , "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead," *Communications Surveys & Tutorials, IEEE* , vol.14, no.2, pp.355-379, Second Quarter 2012.

[38] L. B. Michael, M. J. Mihaljevic, S. Haruyama, and R. Kohno. A framework for secure download for software-defined radio. *IEEE Communications Magazine*, July 2002.

[39] E. Gallery and C. Mitchell, “Trusted computing technologies and their use in the provision of high assurance SDR platforms,” in *2006 Software Defined Radio Technical Conf. Product Exposition*, Nov 2006.

[40] Wenkai Wang; Husheng Li; Yan Sun; Zhu Han; , "Attack-proof collaborative spectrum sensing in cognitive radio networks," *Information Sciences and Systems*, 2009. CISS 2009. 43rd Annual Conference on , vol., no., pp.130-134, 18-20 March 2009.

[41] Kei Sakaguchi Chih Fung Lam Tien Dzung Doan Munkhtur Togooch Jun-Ichi Takada Kiyomichi Araki. ACU and RSM Based Radio Spectrum Management for Realization of Flexible Software Defined Radio World. *IEICE Transactions on Communications* Vol.E86-B No.12 pp.3417-3424.

[42] Woo-Yong Choi; , "Clustering Algorithm for Hidden Node Problem In Infrastructure Mode IEEE 802.11 Wireless LANs," *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on ,* vol.2, no., pp.1335-1338, 17-20 Feb. 2008.

[43] Lain-Jinn Hwang; Shiann-Tsong Sheu; Yun-Yen Shih; Yen-Chieh Cheng; , "Grouping strategy for solving hidden node problem in IEEE 802.15.4 LR-WPAN," *Wireless Internet, 2005. Proceedings. First International Conference on* , vol., no., pp. 26- 32, 10-14 July 2005.

[44] Zhu Han; Rongfei Fan; Hai Jiang; "Replacement of spectrum sensing in cognitive radio," *Wireless Communications, IEEE Transactions on* , vol.8, no.6, pp.2819-2826, June 2009.

[45] Zhu Han; Hai Jiang; "Replacement of Spectrum Sensing and Avoidance of Hidden Terminal for Cognitive Radio," *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE* , vol., no., pp.1448-1452, March 31 2008-April 3 2008.

[46] Hussain, S.; Fernando, X.; , "Spectrum sensing in cognitive radio networks: Up-to-date techniques and future challenges," *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference* , vol., no., pp.736-741, 26-27 Sept. 2009.

[47] Nuallain, E.O.; , "A Proposed Propagation-Based Methodology with Which to Address the Hidden Node Problem and Security/Reliability Issues in Cognitive Radio," *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1-5, 12-14 Oct. 2008.

[48] Galindo-Serrano, A.; Giupponi, L.; , "Distributed Q-Learning for Aggregated Interference Control in Cognitive Radio Networks," *Vehicular Technology, IEEE Transactions on* , vol.59, no.4, pp.1823-1834, May 2010.

[49] Derakhshani, M.; Tho Le-Ngoc; , "Aggregate Interference and Capacity-Outage Analysis in a Cognitive Radio Network," *Vehicular Technology, IEEE Transactions on* , vol.61, no.1, pp.196-207, Jan. 2012.

[50] Zengmao Chen; Cheng-Xiang Wang; Xuemin Hong; Thompson, J.S.; Vorobyov, S.A.; Xiaohu Ge; Hailin Xiao; Feng Zhao; , "Aggregate Interference Modeling in Cognitive Radio Networks with Power and Contention Control," *Communications, IEEE Transactions on* , vol.60, no.2, pp.456-468, February 2012.

[51] CORAL. http://www.crc.gc.ca/en/html/crc/home/wifi_cr/wifi_cr. Last accessed 30/08/2012.

[52] Sydor, J.; , "CORAL: A WiFi based cognitive radio development platform," *Wireless Communication Systems (ISWCS), 2010 7th International Symposium on* , vol., no., pp.1022-1025, 19-22 Sept. 2010.

[53] Guan Jianxin; Ye Xiaohui; Gao Jun; Liu Quan; , "The Software Communication Architecture specification: Evolution and trends," *Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on* , vol.2, no., pp.341-344, 28-29 Nov. 2009.

Glossary and Definitions

Acronym	Meaning
ACU	Automatic Calibration & certification Unit
CEPT	European Conference of Postal and Telecommunications Administrations
CCC	Cognitive Control Channel
CMMI	Capability Maturity Model Integration
CR	Cognitive Radio
CRN	Cognitive Radio Network
CUS	Collective Use of the Spectrum
DSA	Dynamic Spectrum Access
DTV	Digital TV
DYSPAN	Dynamic Spectrum Access Networks
ETSI	European Telecommunications Standards Institute
EVM	Error Vector Magnitude
FCC	Federal Communications Commission
IDA	Infocomm Development Authority of Singapore
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunication Union
JPEO	Joint Program Executive Office
JTAP	JTRS Test Application
JTEL	JTRS Test and Evaluation Laboratory
JTRS	Joint Tactical Radio System
MAC	Medium Access Control
MIDP	Mobile Information Device Profile
MVNO	Mobile Virtual Network Operator
OTA	Over The Air
PDF	Probability Density Functions
PU	Primary User
R&TTE	Radio and telecommunications terminal equipment
RF	Radio Frequency
REM	Radio Environment Map
REM-SDT	REM-based radio scenario-driven testing
R&TTE	Radio equipment and Telecommunications Terminal Equipment
SDR	Software-Defined Radio

SU	Secondary User
TC	Technical Committee
TCAM	Telecommunications Conformity Assessment and Market Surveillance Committee
TR	Technical Report
TTCN	Testing and Test Control Notation
USRP	Universal Software Radio Peripheral
WiFi	Wireless Fidelity
WNAN	Wireless Network After Next
WPAN	Wireless Personal Area Network
WRC	World Radiocommunication Conference
WSD	White Spaces Devices
xG	Next Generation
XML	Extensible Markup Language