Testbed for Cognitive Radio Networks Based on USRP2/N200 Modules

Roman Marsalek, Demian Lekomtcev
Dept. of Radio electronics
Brno University of Technology
Brno, Czech Republic
email: marsaler@feec.vutbr.cz, xlekom00@stud.feec.vutbr.cz

***Abstract*—This paper deals with description of software defined radio test-bed based on USRP2/N200 modules available from ETTUS research. The aim of this test-bed is to develop and test the algorithms for cognitive radio mobile networks. The primary focus is on the spectrum sensing in moving secondary users scenario, adaptation of the radio resource parameters and evaluation of sensitivity to security threats in the mobile cognitive radio networks. Besides the overall architecture description, the paper presents used way to emulate the signals of various communication and broadcasting systems - designed incumbent system simulator and describes the basic implemented blocks - simple OFDM modem, spectrum sensing based on the cyclic prefix correlation and modified method for OFDM subcarrier allocation adaptation.**

***Keywords-cognitive networks*; *sensing*; *resource allocation*, *attacks*.**

I. INTRODUCTION

The Cognitive radio (CR) idea was introduced by J. Mitola [1] as a promising concept bringing more personalized, reliable and inteligent way of data transmission. The key component of the nowadays cognitive radios is the dynamic spectrum access to improve the spectrum utilization in wireless communications. In such concept, all the cognitive radio users are divided into the primary (PU) and the secondary (SU) users. The primary users hold the rights to access the spectrum resources, while the secondary users scan the frequency spectrum (try to detect a spectrum holes in time or frequency domain) and adapt transmission parameters to actual available communication channel.

The application of cognitive radio principles are currently being included into several standards. As the examples, it is possible to mention the IEEE 802.22 [2], IEEE 802.11af standards or recently started standardization process of IEEE 1900.7.

The critical technical problem of CR is the reliable detection of the primary user's signals. Two main approaches can be considered - spectrum sensing or geolocation. High reliability is required even in case of low signal to noise ratios in order to prevent the interference to incumbent (licensed, primary) users. The spectrum sensing algorithms [10], [3] are often unfortunately not able to provide the required reliability and the decission result is always known with some probability of detection and false alarm probability. The interference of secondary users to primary system has been studied in detail in [9]. Note that up to now, the research of cognitive radio has been primarily oriented to static primary and secondary users. An example of more recent work oriented to mobile scenario is [6]. Besides the theoretical concepts and analysis, the experimental evaluation of cognitive radio principles is in progress on specialized test-beds or on the test-beds created using commercialy available radio modules, like the one using USRP's described in [8].

This paper is structured as follows. Section II describes the HW architecture, Section III presents the SW architecture and the basic security threats are described in the Section IV. The paper is summarized in Section V.

II. HW AND ARCHITECTURAL DESCRIPTION

A. General description

Similarly to paper [8], the test-bed under development makes use of commercially available Universal Software Radio Peripheral (USRP) modules, in their current version USRP N200 (eventually we use USRP2). The USRP's can be programmed through a GNU radio, a MATLAB environment or with the use of UHD drivers. As the alternative, it is also possible to use a LabView software produced by National Instruments. The later will be also considered for the future implementation, our current work is made in Simulink/Matlab environment.

According to the general idea, several primary users (PU) share the geographical area with the secondary users. The cellular configuration is assumed. Due to the PU user's mobility, the PU can change its current cell. The secondary users are created using USRPN200 (N210/2) hardware equipped with radio frequency daughtercards. The primary users are created using either the USRP (in its original version) transmitting the signals stored in the memory or FPGA based system is used. Moreover, due to the same OFDM technique used for PU's and SU's, each secondary user can be reconfigured to primary user mode simulating OFDM user defined signals.

Three modes of operation will be possible:

- *Non-cooperative cognitive radio network* (Fig. 1 top) All SU's perform their own spectrum sensing and corresponding channel allocation and OFDM parameter optimization

 ISBN: 978-1-61208-197-7

- *Cooperative cognitive radio network with centralized fusion center* (Fig. 1 middle part)
  The SU's perform the spectrum sensing operation and send the results to the fusion center that makes decision on the channel assignment. This fusion center could be either one for the whole network of secondary users or several fusion centers will be used - each for one cognitive radio *cell*.
- *Cooperative cognitive radio network with decentralized information sharing* (Fig. 1 bottom)
  The SU's perform the spectrum sensing and share the information within their geographical neighbors.

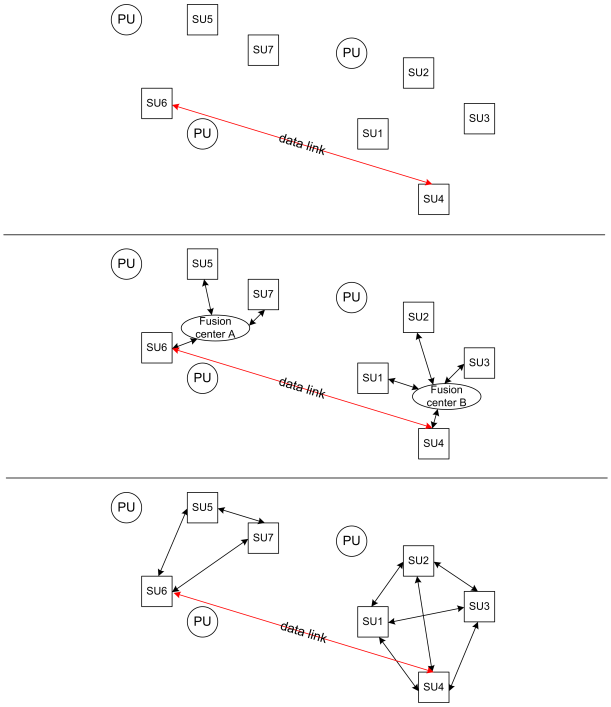

Figure 1. Modes of operation

For the practical experiments, two possible cases are expected. Prior to the wireless implementation, the wired implementation using the basic LFRx and LFTx daughterboards is developed, according to the Fig. 2. Its advantage is that all the signals are connected via the coaxial cables and thus it is possible to achieve perfectly controlled system behavior. Moreover, the two channels - communication between the secondary users and the fusion center (dashed lines) and data channel (solid lines) are perfectly separated and thus there is no need to switch between the channels by mean of the time division duplexing. The channels *A* of the LFTx/LFRx boards are reserved for the communication between the nodes and the fusion center, while the channels *B* are used for the data transfer and spectrum sensing of the incumbent users. The data transmission is monitored by the Rohde & Schwarz spectrum analyzer FSQ3. After the tests with this first setup, the system is going to be changed to the completely wireless solution. For such setup, the USRP daughterboards LFRx, LFTx will be replaced by the SBX (400MHz-4.4GHz) or RFX2400 (2.3-2.9GHz) daughterboards and the operation will be in the 2.4GHz ISM band. In such a case, both the data transfer and communication between the nodes and the fusion center is going to proceed through the radio channel according to the schematic on Fig. 4.

B. Incumbent system simulator

In order to check the functionality of system behavior and especially sensing methods for various primary user signals, the FPGA-based incumbent simulator has been created with the use of the Xtreme DSP Starter kit - a Spartan 3A-DSP board from Xilinx. According to the selected standard, the FPGA continualy loads the data from the memory and converts the samples with the D/A converter to the analog domain. These signals were generated using the vector signal generator SMU200 as a data source, see Fig. 3. The data were captured with the CompuScope 12400 high-speed sampling card into the MATLAB environment. Subsequently, data were converted to the Q15 format suitable for the FPGA implementation.

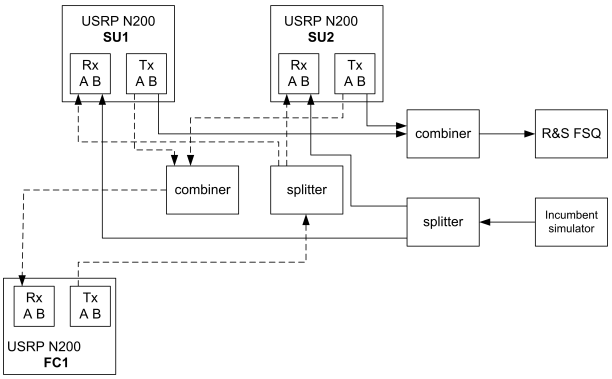

Figure 2. First experiment use-case: wired experimental solution

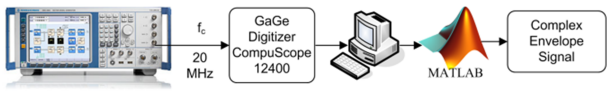

Figure 3. Incumbent signals capture setup

 ISBN: 978-1-61208-197-7

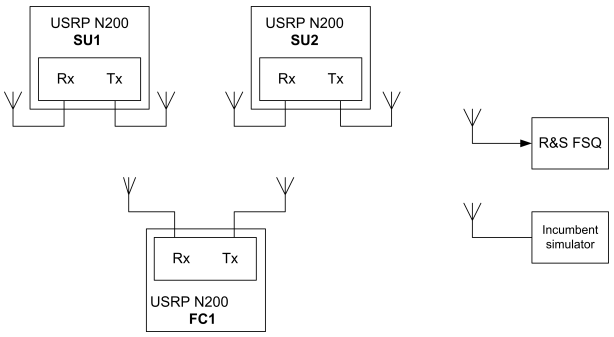

Figure 4. Second experiment use-case: wireless experimental solution

III. SW ARCHITECTURE AND ALGORITHMS

A. PHY layer parameters

The selected approach allows the use of OFDM/OFDMA in both PU and SU network. The principle of an Orthogonal Frequency Division Multiplexing (OFDM), belonging to the family of multicarrier transmission is currently widely used in Local Area Networks (WiFI 802.11.a,g), digital broadcasting (DVB-T, DAB) or wireless mobile communication systems (LTE/LTE-A). Moreover it is also a candidate for cognitive radio defined by the IEEE 802.22 standard [2]. The reason lies in its immunity to multipath propagation and high flexibility of the physical layer. On the contrary, the OFDM suffers from high Peak to Average Power Ratio or sensitivity to transceiver imperfections. The use of OFDM in primary user networks well corresponds with the future deployment of LTE network.

1) Secondary user signals: The OFDM is supposed for the secondary user data transmission. The maximum signal bandwidth is limited to $B_{tot} = 8$MHz (initially motivated by the one TV channel bandwidth), divided into ten B_{sb} =750 kHz wide subblocks. In each subblock, N =12 subcarriers (with the FFT length of 16) can be loaded with BPSK or QPSK data, that results in the subcarrier separation $\Delta f = 62.5$ kHz and the useful OFDM symbol duration $T_u = 1/\Delta f = 16\mu s$. A cyclic prefix of the length $T_{cp} = 4\mu$ s. is added resulting to the total OFDM symbol duration of 20 μs. The bit-rate for one subblock is then 1.25 Mbit/s in QPSK mode. Prior to the OFDM data transmission, a quiet period of duration $T_{quiet} = 20\mu s$. (period within the spectrum sensing, decision and radio resource allocation reconfiguration is done) preceeds. During the tests, the variable number of OFDM symbols can be sent in successive way as shown in the timing structure on Fig. 5. The schematics of the implemented basic OFDM modulator and demodulator are shown in Fig. 6. In the modulator, the input of the IFFT block is first created from the data and zero subcarriers. Subsequently, the cyclic prefix is added. The operations of the demodulator are performed in the inverse order.

2) Incumbent signals: As mentioned above, additionally to the OFDM based primary user signals, other incumbent signal types can be used for the test purposes including DVB-T (8 MHz bandwidth), WiMax (1.75MHz bandwidth), GSM/GSM-EDGE (200 kHz bandwidth) and custom-defined single-carrier (BPSK, QPSK, M-QAM) and custom-defined multicarrier OFDM signals (both up to 8 MHz bandwidth).

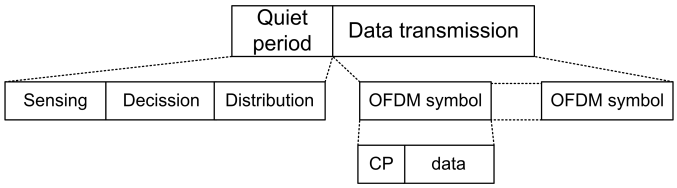

Figure 5. Timing structure for the OFDM communication and sensing

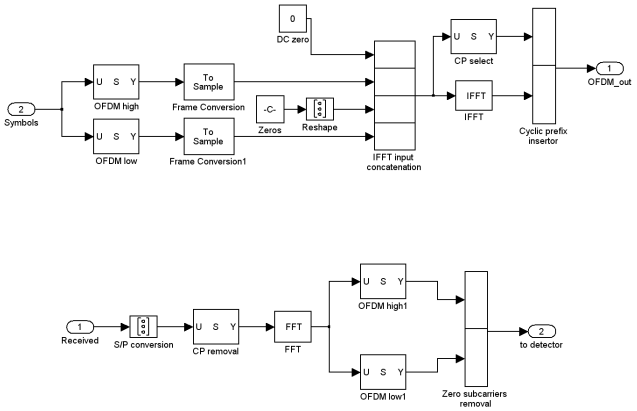

Figure 6. The schematic of basic implementation of OFDM modulator (top) and demodulator (bottom)

B. Resource allocation

In order to increase the Quality of Service, the adaptive OFDM has been proposed in the past [5]. Several methods have been proposed in order to optimize the OFDM parameters. The most straightforward method is to optimize the modulation order on the individual OFDM subcarriers - called adaptive bit-loading. Several waterfilling-based methods exist and were used with slight modifications [12]. Their application in wireless communications results in the effective channel use, but at the expense of the complexity and need for either channel estimation or bit error rate estimation. In our architecture, a modification of basic bit-filling greedy algorithm [11] that iteratively assigns one bit at a time to the selected subcarrier has been implemented with the use of Simulink environment. If the n-th subcarrier already carries b_n bits, the power ΔP_n^+ needed to transmit

 ISBN: 978-1-61208-197-7

one additional bit is given by:

$$\Delta P_n^+ = \frac{2^{b_n}}{g_n}, \quad (1)$$

where g_n is the channel gain to noise ratio of the n-th subcarrier defined by:

$$g_n = \frac{|H_n|^2}{N_n}. \quad (2)$$

Here H_n denotes the channel frequency response and N_n is the noise power. The Error Vector Magnitude parameter (EVM, [14]) measurement is used in order to eliminate the channel estimation part in eq. 2 as it holds that $\text{SNR}_n = \frac{|H_n|^2}{N_n} P_n$, where P_n is the power allocated to the n-th subcarrier. In condition of the equal allocated power on all subcarriers ($P_n = P, \quad \forall n$), the SNR is equivalent to the channel gain to noise ratio from eq. 2 and the value of EVM on the n-th subcarrier EVM_n could approximate the channel gain to noise ratio:

$$g_n \approx \frac{1}{\text{EVM}^2}. \quad (3)$$

C. Spectrum sensing

The spectrum sensing can be understood as the detection problem with two hypothesis. The first hypothesis H_0 assumes the presence of noise only, while the second hypothesis H_1 assumes the reception of primary user's signal corrupted by the additive noise component. Many methods have been already investigated as:

- energy detector
- cyclostationary detector
- cyclic prefix correlation for OFDM
- matched filter detector
- eigenvalue detector
- statistical tests like Kolmogorov-Smirnov etc.

The simplest method of spectrum sensing is the energy detector that we implemented in Simulink environment and that will be used in the test-bed as the first choice of detectors for the detection of presence of non-OFDM signals. Performance of other, more complex, detectors depends on the properties of detected primary signals. As the OFDM/OFDMA is planned to be used for both PU and SU, the cyclic prefix correlation can be used, or alternatively a cyclostationarity detector can be employed. These approaches can be effectively used in both DVB-T whitespaces or in the LTE band. The results of previous experiments can be found e.g. in our previous paper [13]. For the primary users transmitting with the OFDM signals, we implemented in Matlab the simple cyclic prefix correlation method for signal detection. As shown in Fig. 7, two sliding windows of the width T_{cp} separated by $T_u - T_{cp}$ are moved along the time and the correlation among them is computed. This principle is the same as for the initial phase of OFDM symbol synchronization so the HW parts can be reused. Unlike in the case of fixed cognitive radio network, the spectrum sensing (or equivalently database access) has to be repeated regularly by the secondary user nodes in order to get the realistic overview on spectrum usage situation. This is the reason for the quiet period we defined above.

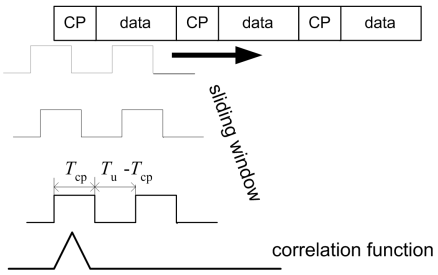

Figure 7. Sliding window correlation for OFDM signals spectrum sensing

The principle of secondary user operation will be as follows. In the first part of operation (quiet period as required for IEEE 1900.7 standard call), the secondary users scan the channel situation using an sensing frontend (in the future an alternative approach - geolocation will be also used or combined with sensing). After the analysis by the signal processing methods, the total bandwidth allocated to the secondary users will be distributed among all SU nodes in order to minimize the interferences to PU's and required total transmitted power. The OFDM resource allocation will subsequently be performed according to the EVM parameter as in [12].

IV. Cognitive radio attacks

It is expected that in future cognitive radio network, security will be an important issue as a result of attacks specific to dynamic spectrum access and resource adaptation. Several possible attacks have been identified in the literature (see [4] as example) as the PU emulation attacks, spectrum honeypots, spectrum handoff attacks, objective function attacks, byzantine failure in distributed spectrum sensing, etc. The basic technique to attack the cognitive radio network is the PU emulation, when the malicious unlicensed user emulates the characteristics of primary users.

The defense against the objective function attacks has been proposed in [15]. One of the simplest approaches to mitigate the PU emulation problem is to consider the stationary character of primary users, often being a static TV towers, [4]. Another approach is the usage of so called *helper nodes* - devices geographically spread over the PU area responsible for the authentication process [7] transmitting the spectrum status information. In future networks, the mobility of users (both primary, but at least secondary users) will be required. Thus, some more advanced methods have to be investigated that will be important part of future

 ISBN: 978-1-61208-197-7

research. The proposed test-bed will be used for the practical experiments with the cognitive radio networks security - including the attacks to helper nodes or primary signal emulation attacks.

V. Summary and perspectives

In this paper, we described a cognitive radio test-bed that is currently under development for test of cognitive radio physical layer algorithms, access techniques and emulation of cognitive radio network under attacks of malicious users. Both the primary and secondary users are going to employ an OFDM transmission scheme and the mobility of the secondary users (in future also of the primary) will be expected in the final version. The main parameters of the designed OFDM system, the implementation of basic modem and description of the blocks used for spectrum sensing and resource allocation is presented in the paper.

VI. Acknowledgments

Research described in this paper received funding by the Czech Science Foundation project no. 102/09/0776 and by the Brno University of Technology internal project FEKT-S-11-12 (*MOBYS*). It is performed in laboratories supported by the *SIX* project; no. CZ.1.05/2.1.00/03.0072, the operational program Research and Development for Innovation. The support of the project CZ.1.07/2.3.00/20.0007 *WICOMT*, financed from the operational program Education for Competitiveness, is also gratefully acknowledged. The cooperation in the COST IC1004 action was supported by the MEYS of the Czech Republic project no. LD12006 (*CEEC*).

References

[1] J. Mitola III and G.Q. Maguire, Cognitive Radios: Making Software Radios more Personal. *IEEE Personal Communications*, vol. 6, no. 4, Aug. 1999, pp. 13-18.

[2] C. Cordeiro, K. Challapali, D. Birru, and S.N. Shankar, IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios. *Journal of Communications*, April 2006, vol. 1, no. 1, pp. 38 - 47.

[3] S. Pollin, L. Hollevoet, F. Naessens, P. Van Wesemael, A. Dejonghe, and L. Van der Perre, "Versatile Sensing for Mobile Devices", *Proceedings of the 3rd ACM workshop on Cognitive radio networks - CoRoNet '11*, Las Vegas, Nevada, USANew York, New York, USA, ACM Press, 08/2011, pp. 1-6.

[4] T.C. Clancy and N. Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, 15-17 May 2008, ISBN: 978-1-4244-2301-9, pp. 1 - 8.

[5] A. Czylwik, Adaptive OFDM for wideband radio channels, In *Proceedings of Global Telecommunications Conference GLOBECOM '96*, Vol. 1, Nov. 1996, pp. 713 - 718.

[6] A. W. Min, K.-H. Kim, J. P. Singh, and K. G. Shin, Opportunistic Spectrum Access for Mobile Cognitive Radios, *in Proc. of the 30th IEEE Conference on Computer Communications (IEEE INFOCOM 2011)*, Shanghai, China, April 2011, pp. 2993 - 3001.

[7] S. Chandrashekar and L. Lazos, A Primary User authentication system for mobile cognitive radio networks, *In Proc. of Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium*, 7-10 Nov. 2010, ISBN: 978-1-4244-8131-6, pp. 1 - 5.

[8] Z. Yan, Z. Ma, H. Cao, G. Li, and W. Wang, Spectrum Sensing, Access and Coexistence Testbed for Cognitive Radio using USRP, *In proc. of Circuits and Systems for Communications, 2008. ICCSC 2008. 4th IEEE International Conference on*, 26-28 May 2008, ISBN: 978-1-4244-1707-0, pp. 270 - 274.

[9] J. Kerttula and R. Jantti, DVB-T Receiver Performance Measurements Under Secondary System Interference, *In Proc. of The First International Conference on Advances in Cognitive Radio (COCORA 2011)*, April 17-22, 2011 - Budapest, Hungary. pp. 76-80.

[10] T. Yucek and H. Arslan, A Survey of Spectrum Sensing Algorithms for Cognitive Radiao Applications. *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, First Quarter 2009, pp. 116 130.

[11] N. Papandreou and T. Antonakopoulos, Bit and Power Allocation in Constrained Multicarrier Systems: The Single-User Case, *Eurasip Journal on Advances in Signal Processing*, Vol. 2008, ISSN:1110-8657, pp. 1-14.

[12] R. Marsalek, K. Povalac, and J. Dvorak, Use of The Error Vector Magnitude for low-complex bit loading in Orthogonal Frequency Division Multiplexing, In *Proc. of 7th International Symposium on Image and Signal Processing and Analysis (ISPA 2011)* September 4-6, 2011, Dubrovnik, Croatia, pp. 42-45.

[13] P. Sramek, J. Svobodova, R. Marsalek, and A. Prokes, Using Cyclic Prefix Correlation for DVB- T Signals Detection. In *ICECom 2010 20th International Conference on Applied Electromagnetics and Communications Conference Proceedings*. Dubrovnik: KOREMA, 2010, ISBN: 978-953-6037-58- 2, pp. 1-4.

[14] M.D. McKinley, K.A. Remley, M. Myslinski, J.S. Kenney, D. Schreurs, and B. Nauwelaers, EVM Calculation for Broadband Modulated Signals. In *Proceedings of the 64th ARFTG Microwave Measurements Conference*, Orlando, FL, 2 - 3 December, 2004, ISBN: 0-7803-8952-2, pp. 45-52.

[15] Q. Pei, H. Li, J. Ma, and K. Fan, Defense Against Objective Function Attacks in Cognitive Radio Networks, Chinese Journal of Electronics, Vol.20, No.4, Jan. 2011, pp. 138-142

 ISBN: 978-1-61208-197-7