IARIA

COCORA 2015

The Fifth International Conference on Advances in Cognitive Radio

ISBN: 978-1-61208-403-9

April 19 - 24, 2015

Barcelona, Spain

COCORA 2015 Editors

Tibor Gyires, Illinois State University, USA

COCORA 2015

Foreword

The Fifth International Conference on Advances in Cognitive Radio (COCORA 2015), held between April 19th-24th, 2015 in Barcelona, Spain, continued a series of events dealing with various aspects, advanced solutions and challenges in cognitive (and collaborative) radio networks. It covered fundamentals on cognitive and collaborative radio, specific mechanism and protocols, signal processing and dedicated devices, measurements and applications.

Most of the national and cross-national boards (FCC, European Commission) had/have a series of activities in the technical, economic, and regulatory domains in searching for better spectrum management policies and techniques, due to spectrum scarcity and spectrum underutilization issues. Therefore, dynamic spectrum management via cognition capability can make opportunistic spectrum access possible (either by knowledge management mechanisms or by spectrum sensing functionality). The main challenge for a cognitive radio is to detect the existence of primary users reliably in order to minimize the interference to licensed communications. Optimized collaborative spectrum sensing schemes give better spectrum sensing performance. Effects as hidden node, shadowing, fading lead to uncertainties in a channel; collaboration has been proposed as a solution. However, traffic overhead and other management aspects require enhanced collaboration techniques and mechanisms for a more realistic cognitive radio networking.

We take here the opportunity to warmly thank all the members of the COCORA 2015 Technical Program Committee. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to COCORA 2015. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the COCORA 2015 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that COCORA 2015 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of cognitive radio.

We also hope Barcelona provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful city.

COCORA 2015 Advisory Committee:

Tomohiko Taniguchi, Fujitsu Laboratories Limited, Japan
Adrian Popescu, Blekinge Institute of Technology - Karlskrona, Sweden
Alan A. Varghese, Coherent Logix, USA

COCORA 2015

Committee

COCORA Advisory Committee

Tomohiko Taniguchi, Fujitsu Laboratories Limited, Japan
Adrian Popescu, Blekinge Institute of Technology - Karlskrona, Sweden
Alan A. Varghese, Coherent Logix, USA

COCORA 2015 Technical Program Committee

Anwer Al-Dulaimi, Brunel University, UK
Annamalai Annamalai, Prairie View A&M University, USA
Cornelia Badoi, Microsoft, Romania
Ilham Benyahia, Université du Québec en Outaouais, Canada
Derya Çavdar, Bogazici University, Istanbul, Turkey
Lingjie Duan, Singapore University of Technology and Design, Singapore
Malgorzata Gajewska, Gdansk University of Technology, Poland
Slawomir Gajewski, Gdansk University of Technology, Poland
Matthieu Gautier, Université de Rennes 1, IRISA, INRIA, France
Liljana Gavrilovska, Ss. Cyril and Methodius University -Skopje, Macedonia
Tien-Ke Huang, National Tsing Hua University, Taiwan
Abubakar Sadiq Hussaini, Instituto de Telecomunicações - Aveiro, Portugal | American University of Nigeria, Nigeria
Muhammad Umar Khan, Center for Advanced Studies in Telecommunication (CAST), Pakistan
Insoo Koo, University of Ulsan, South Korea
Thomas D. Lagkas, International Faculty of the University of Sheffield, CITY College, Greece
Jia-Chin Lin, National Central University, Taiwan
Marco Listanti, University of Rome La Sapienza, Italy
Ivana Maric, Ericsson Research in San Jose, USA
Jean-Claude Moissinac, TELECOM ParisTech, France
Homayoun Nikookar, Delft University of Technology, The Netherlands
Sema Oktug, Istanbul Technical University, Turkey
Adrian Popescu, Blekinge Institute of Technology - Karlskrona, Sweden
Arnd-Ragnar Rhiemeier, Cassidian Electronics - Ulm, Germany
Mario Eduardo Rivero Angeles, Computation Research Center (CIC-IPN), Mexico
Daniel Riviello, Politecnico di Torino, Italy
Usman Shahid, NDSU - Fargo, USA
Boyan Soubachov, University of Cape Town, South Africa
Silvian Spiridon, Broadcom - Bunnik, The Netherlands
Marko Suojanen, Finnish Defence Research Agency, Finland
Tomohiko Taniguchi, Fujitsu Laboratories Limited, Japan
Alan A. Varghese, Coherent Logix, USA
Liaoyuan Zeng, University of Electronic Science and Technology of China, China

Copyright Information

Table of Contents

Security Aspects in Cognitive Radio Networks

Detection and Mitigation of Primary User Emulation Attacks

Mahmod Ammar, Nick Riley, Meftah Mehdawi, Anwar Fanan, Mahsa Zolfaghari

School of Engineering
University of Hull
Hull, UK
E-mails: {M.A.Ammar@2011, N.G.riley, M.A.Mehdawi@2010, A.M.Fanan@2012, M.Zolfaghari@2009}.hull.ac.uk

***Abstract*—Cognitive Radio Networks (CR) is an advanced growing technique and a promising technology for the upcoming generation of the wireless networks. Deployment of such networks is hindered by the vulnerabilities that these networks are exposed to, in this paper we focus on security problems arising from Primary User Emulation Attacks (PUEA) in CR networks. We study the impact of this attack on CR networks, detection and defense approaches. We have setup the system model using Matlab software; the Neyman-Pearson composite hypothesis test NPCHT is used to obtain the hypothesis test and detect the PUEA. Simulation results proved that using NPCHT it is possible to keep the probability of successful PUEA low, and this depends on the threshold values; the number of malicious users in the system can significantly increase the probability of false alarm in the network, Also it shows that there is a range of network radii in which PUEA are most successful.**

Keywords-Cognitive Radio (CR); Primary User Emulation Attack (PUEA); Probability Density Function (PDF); Neyman Pearson composite hypothesis test (NPCHT);

I. INTRODUCTION

Spectrum sensing and spectrum sharing are important functionalities of CR which enables the secondary users to monitor the frequency spectrum and detect vacant channels to use [1]; it is also important to address the security and reliability issues in the CR. An example of CR networks is the usage of unused spectrum (white spaces) in the television band where the TV transmitter becomes a primary transmitter, i.e., the TV receivers are primary receivers or licensed users and while the other users who are not TV subscribers but wish to use the spectrum in the TV band for their own communication becomes secondary transmitters/receivers.

The essential purpose of spectrum sensing employment in a CR network is to identify empty spectral bands (white spaces) and once these white spaces have been identified, CR nodes opportunistically utilize these unoccupied bands of spectrum by wirelessly operating across them while simultaneously avoiding interference with the primary users [2]. In a CR network, primary users possess the priority to access the spectrum band, while the secondary users must always give up access of the spectrum band over to the primary users and ensure that no interference is caused. Subsequently, if a primary user begins to transmit across a frequency band occupied by a secondary user, the secondary user is ideally required to vacate that specific spectral band immediately. But when there is no active primary user communication in the spectrum, all other users enjoy equal right to access the unoccupied spectrum band. For a secondary user to gain equal rights as the primary user, the secondary user may tend to modify the air interface so as to mimic the primary user's characteristics causing the secondary user to behave maliciously. The resultant effect of this is that the other secondary users will identify the malicious user as a primary user there by vacating the occupied spectrum band for the malicious user believing that it is a primary user. In this way, the malicious user gets access to the primary user's spectrum band. In literature, this kind of attack against CR networks is considered as a Primary User Emulation Attack (PUEA) [3].

Therefore, we can define PUEA as an attack in CR networks where the malicious user pretends to be the primary user to obstruct idle channels by transmitting a similar signal as the primary user [3]. Masquerading of a primary user allows threat identifies the malicious masquerading of a primary user like a digital TV broadcaster. The malicious attacker may mimic the primary user characteristics in a specific frequency band (e.g., white space band), so that the legitimate secondary users erroneously identify the attacker as an incumbent and they avoid using that frequency band; the attacker primary focus is to disrupt the secondary user's transmissions by making contact with it as many times as possible, each time the jammer does this it forces the secondary users to change channels as they cannot differentiate it from a primary user. The presence of PUEA causes a number of troubles for CR networks. A PUEA can be launched while the spectrum is being sensed or detected by using cyclostationary, energy or matched filter detection signal features [4].

We can classify the protection techniques against these types of threats in the following categories: (i) protection techniques based on reputation and trust of the CR nodes [5], (ii) identification of the masquerading threat though signal analysis [6], (iii) authentication of the CR node through cryptographic techniques [7], and (iv) geolocation database of primary users [8].

The remainder of this paper is organized as follows. In Section II, the model design and simulation setup are Introduced. Section III describes the model analysis and probability density function of the received signal. Our simulation results, conclusion and future work are discussed in Section IV and section V, respectively.

A. Objective of adversarial attackers

The objectives of an attacker have a direct correlation with the way the attacks are launched, and therefore, they determine the nature of attacks [9][10].

1) *Selfish attacks*: The attacker's motive is to acquire more spectrum for its own use by preventing others from competing for the channels and unfairly occupying their share. In this type of attack, adversaries will defy the protocols and policies only if they are able to benefit from them [11][12].

2*) Malicious attacks:* The attacker's only objective is to create hindrance for others and does not necessarily aim at maximizing own benefits. They do not have any rational objective and identify protocols and policies to just induce losses to others [13].

B. Impact of PUE attacks on CR Networks

The presence of PUE attacks causes a number of troubles for CR networks. The list of potential consequences of PUE attacks is:

- Bandwidth waste: The ultimate objective of deploying CR networks is to address the spectrum under-utilization that is caused by the current fixed spectrum usage policy. By dynamically accessing the spectrum "holes", the SUs are able to retrieve these otherwise wasted spectrum resources [14].
- QoS degradation: The appearance of a PUE attack may severely degrade the Quality-of-Service (QoS) of the CR network by destroying the continuity of secondary services [14].
- Connection unreliability: If a real-time secondary service is attacked by a PUE attacker and finds no available channel when performing spectrum handoff, the service has to be dropped. This real time service is then terminated due to the PUE attack. In principle, the secondary services in CR networks inherently have no guarantee that they will have stable radio resource because of the nature of dynamic spectrum access. The existence of PUE attacks significantly increases the connection unreliability of CR networks. Also the Hidden Node Problem (HNP) can cause unreliable connection; the most common approach against HNP is based on collaborative sensing to identify the incorrect spectrum perception of the affected CR node. This is the approach adopted in standard IEEE 802.22 [15], where decision rules (e.g., voting algorithm) are used to correct errors in the spectrum sensing function. In a similar way, this approach is also described by Prasad [16], even if the term distributed spectrum sensing is used.
- Denial of Service: Consider PUE attacks with high Attacking frequency; then the attackers may occupy many of the spectrum opportunities. The SUs will have insufficient bandwidth for their transmissions, and hence, some of the SU services will be interrupted. In the worst case, the CR network may even find no channels to set up a common control channel for delivering the control and this is called Denial of Service in CR networks.

II. MODEL DESIGN AND SIMULATION SETUP

In our scenario, all secondary and malicious users are distributed in a circular grid of radius R, as shown in Fig. 1.

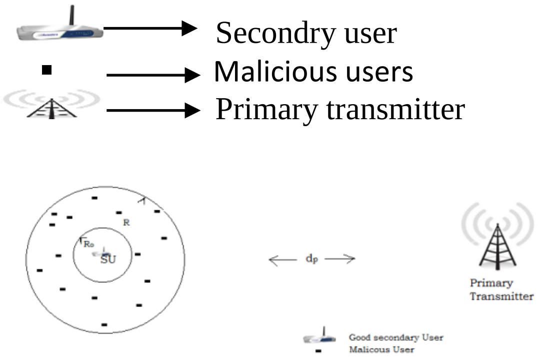

Figure 1. CR Network Model

A primary user (e.g., a TV tower), is located at some distance from all the users, the secondary users are randomly and uniformly distributed within a network radius from the primary transmitter. In order to detect the white spaces or the return of the primary, the secondary users measure the received power, if the received power is below a specified threshold then the spectrum band is considered to be vacant (white space). If the received power is above the specified threshold, then based on the measured power, a decision is made as to whether the received signal was transmitted by a primary transmitter or by a set of malicious users [17]. We design a Neyman-Pearson Composite Hypothesis Test (NPCHT) to obtain a criterion for making this decision. To perform the analysis, the assumptions below are taken:

- ➢ The distance between primary transmitter and all the users is d*p*=120Km.
- ➢ There are M malicious users in the system. M is a geometrically distributed random variable.
- ➢ The locations of malicious users are uniformly distributed in the circular grid of radius R=500m as our simulation shows in Fig. 2 when M=30.The received power at the secondary user from each of the malicious user is Independently and Identically Distributed (IID). This is valid due to the symmetry of the system and the fact that the malicious users presented uniformly in an annular region between the centered at (0, 0) and radii (R_0, R), if the received power is not IID, then the SU will use another power control scheme.

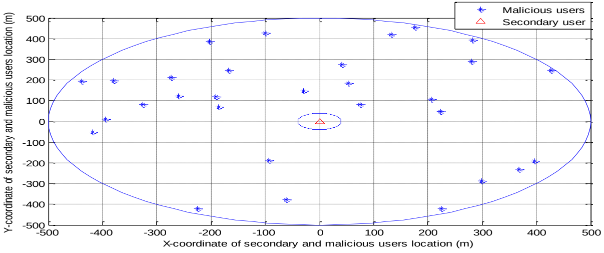

Figure 2. Simulation result of malicious users distributed randomlly around the secondary user located at coordinate (0,0).

- ➢ The primary transmits at a power Pt =120 KW while the malicious users transmit at a power Pm=

5W. All the values of the system parameters we have used are in Table I below.

- The primary transmitter co=ordinates are fixed at a point (rp, θp) and this position is known to all the users in the grid.
- The secondary user co-ordinates (r, θ), no malicious users are present within a circle of radius R0=40m known as "exclusive distance from the secondary user" centered at (r, θ).in case of this condition is not met then the received power at the secondary due to transmission from any subset of malicious users present within a distance R0 from the secondary becomes too large to create PUEA [17].

TABLE I. SYSTEM PARAMETERS FOR OUR SIMULATION

Parameter	Value
Dp: Distance between primary transmitter and other users	120 Km
R : Radius of the circular grid	500 m
R0: Radii of annular region	40 m
M : Number of malicious usres in the system	10,15,30
Pt : Primary transmition power	120 KW
Pm : Malicious transmition power	5 W
σp: : Variance of Primary users	8 dB
σm : Variance of Malicious users	5.5 dB

- The transmission from primary transmitter and malicious users undergo path loss and log normal shadowing with mean 0 and variance σ^2p and σ^2m, respectively [18].
- The path loss exponent chosen for transmission from primary transmitter is 2 and from malicious user are 4.

III. MODEL ANALYSIS AND PROBABILITY DENSITY FUNCTION OF THE RECEIVED SIGNAL:

First, we have to obtain the Probability Density Function (PDF) of the received power at the secondary user due to transmission by the primary and by the malicious users in order to obtain a hypothesis test using Neyman-Pearson composite hypothesis test NPCHT [18].

A. Probability Density Function of the Received Signal

One of the applications of the probability density function of the received power is using it in Neyman Pearson's Composite Hypothesis Test NPCHT or any other statistical test to identify intruders and impostors in CR networks and also investigate the impact of PUEA in the network.

We consider M malicious users located at co-ordinates (rj, θj) 1 ⩽ j ⩽ M. Since the position of the jth malicious user is uniformly distributed in the annular region between R0 and R, rj and θj are statistically independent ∀ j. The pdf of rj , p(rj) ∀ j is given by

$$p(r_j) = \begin{cases} \dfrac{2r_j}{R^2 - R_0^2} & r_j \in [R_0, \ R] \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

where θj is uniformly distributed in (−π,π) ∀j [19]. The received power at a secondary user from the primary transmitter, $p_r^{(p)}$ is given by

$$p_r^{(p)} = P_t d_p^{-2} G_p^2 \tag{2}$$

where $G_p^2 = 10^{\varepsilon p/10}$ and $\varepsilon_p = N(0, \sigma_p^2)$, as mentioned in Section II. Since P_t and d_p are fixed, the pdf of $p_r^{(p)}$, $p^{\mathrm{Pr}}(\gamma)$, follows a log-normal distribution and can be written

$$p^{\mathrm{Pr}}(\gamma) = \frac{1}{A\sigma_{\mathrm{p}}\sqrt{2\pi\gamma}} \exp\left(-\frac{(10\log_{10}\gamma - \mu_p)^2}{2\sigma_p^2} \right) \tag{3}$$

where $A = \frac{\ln 10}{10}$ and $\mu_p = 10\log_{10} p_t - 20\log_{10} d_p$

The total received power at the secondary node from all the M malicious users is given by

$$P_r^{(m)} = \sum_{j=1}^{M} p_m d_j^{-4} G_j^2 \tag{4}$$

where dj is the distance between the jth malicious user and the secondary user and G^2_j is the shadowing between the jth malicious user and the secondary user.

B. Detecting PUEA using Neyman-Pearson Criterion

We have used the two hypotheses in Neyman-Pearson decision criterion, which are given as below:
M1 : Primary Transmission in progress
M2 : Emulation attack in progress
In this hypothesis test, there are two types of errors that secondary user can make [20]:
False alarm: The secondary makes a decision that the transmission is due to primary but the malicious user is transmitting.
Miss Detection: The secondary makes a decision that the transmission is due to malicious user but the primary is transmitting.
In our simulation, the power of the received signal is measured in order to calculate the decision variable which is given by the ratio of Λ= $p^m(\chi)$ / $p^{\mathrm{Pr}}(\chi)$
where $p^{\mathrm{Pr}}(\chi)$ and $p^m(\chi)$ is the pdf of received power from the primary and from all malicious users respectively. Λ is then compared with predefined threshold and the secondary decides the following

$$\Lambda \le \lambda \quad \Longrightarrow \quad \text{D1: Primary transmission}$$

$$\Lambda \ge \lambda \quad \Longrightarrow \quad \text{D2: PUEA in progress}$$

First, secondary user may decide D2 when M1 is true, and second secondary user may decide that D1 when M2 is true. Each of these errors has a probability associated with it which depends on the decision rule and condition densities [14]. Miss Probability: P{D2|M1}= Probability of making decision D2 when M1 is true.
False Alarm Probability: P{D1|M2}=Probability of making decision D1 when M2 is true.

C. Decision Rule

In Fig. 3, we plot the decision rule showing Miss Probability and Probability of false alarm under Gaussian distribution. It shows the two conditional densities of the power received by the good secondary user from primary and malicious transmitters.

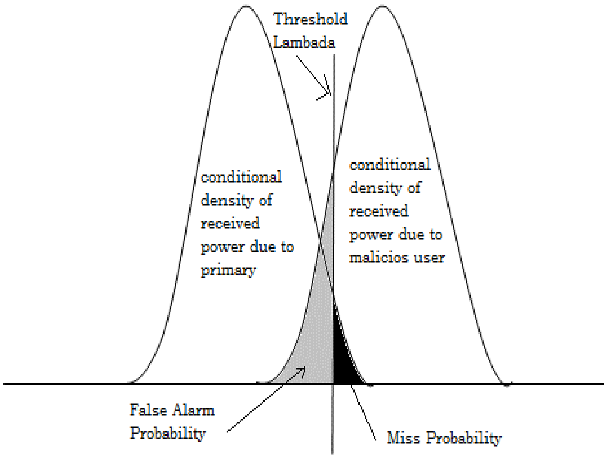

Figure 3. The Decision Rule

We compare the decision rule with the threshold value; Lambda (λ) and the miss probability and probability of false alarm are calculated accordingly [21].

IV. RESULTS AND ANALYSIS

In this section, we present the results obtained using Matlab simulation and also the theoretical results for the similar setup for the probability density function of the received power at the secondary user due to the primary transmitter and the received power at the secondary user due to the malicious users.

Also, we determined the performance of the network for PUE attack in terms of probability of miss detection and false alarm, in addition to the relationship between the false alarm probability (i.e., the probability of successful PUEA) and the network Radius R.

In our simulation, we have used the following system parameters, as shown in Table II.

TABLE II. SYSTEM SIMULATION PARAMETERS

Parameter	dp	R	Ro	M	Pt	Pm	σp	σm
Value	120 KM	500 m	40 m	15	120 KW	5 W	8 dB	5.5 dB

We can see from Fig. 4 and Fig. 5 that the results of the probability density function using simulations considerably match with the one derived mathematically.

There is a slight mismatch and the reason behind this is duo that the theoretical derivation is for ideal setup and over an unlimited duration of time while the simulation testing times are limited in number and also have random effects as per the simulation settings.

It is clear that the probability density functions of the received power at the secondary user from the primary transmitter differ from the received power at the secondary user from the malicious user.

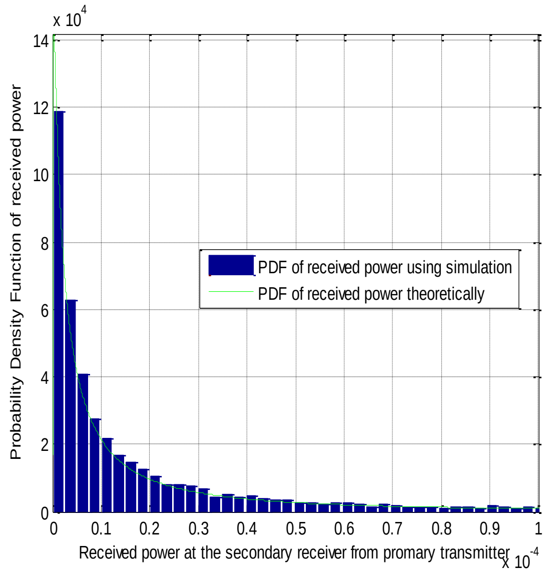

Figure 4. PDF of the received power deu to the primary transmitter

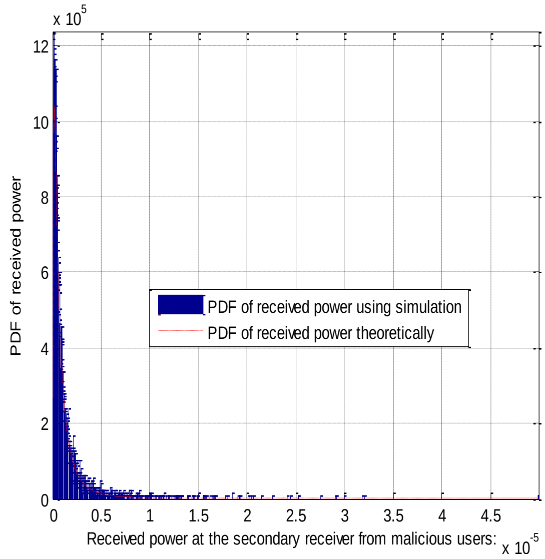

Figure 5. PDF of the received power due to the malicious users

Based on the PDF which we have achieved in our simulation and Neyman Pearson's Composite Hypothesis Test NPCHT approach, we have obtained the probability of successful PUEA (False Alarm),

Fig. 5 shows the relationship between the false alarm probability (i.e., the probability of successful PUEA) and the network Radius R, we set the threshold value λ at 2. It is observed that the probability of false alarm rises and then falls down with increasing value of R and also there is a value of R for which the probability of false alarm is maximum; this is as expected because:

Case 1- for a given R0, if R is small, the malicious users are closer to the secondary user and the total received power from all the malicious users is likely to be larger than that received from the primary transmitter, thus decreasing the probability of successful PUEA.

Case 2- for large R, the cumulative received power at the secondary from the malicious users may not be sufficient to successfully launch PUEA.

We have done the simulation with different values of M, as shown in Fig.6; our results prove that when the PDF is used with NPCHT, the number of malicious users in the system has a significant impact on the network causing the secondary users suffer from degradation in the quality of their communication due to the transmission from the malicious users.

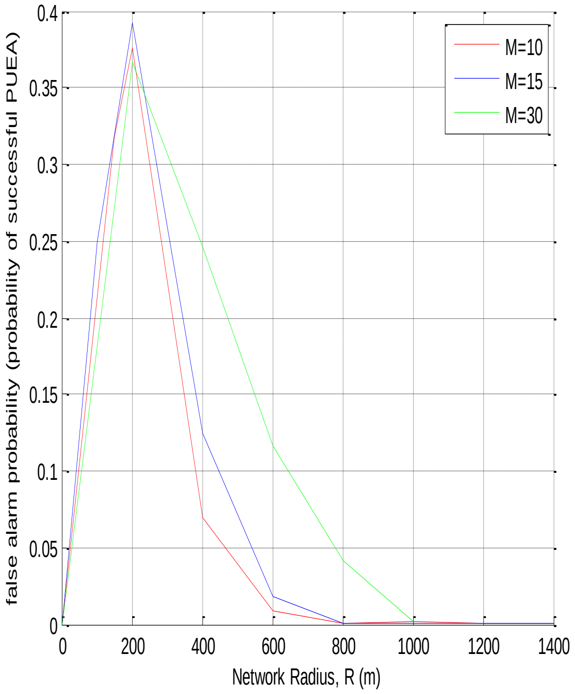

Figure 6. False alarm probability Vs. network Radius R

Fig. 7 and Fig. 8 are the plots for the probability of miss detection vs. the number of simulation times and False alarm vs. the number of simulation times respectively, Probability of miss detection and false alarms are calculated for 600 times of simulations. The threshold value for this simulation is set to 2, i.e. λ=2. The number of malicious users in this case is set to be M=35, the radius of outer region R=400m, Radius of primary exclusive region R0=40m, primary transmitter power Pt=120Kw, malicious transmitter power Pm=5w, σm =5.5dB, σp = 8dB.

As we can see from the experiment, the probability of false alarm (Successful PUEA) is always close to 0.326 (within ±0.04 of this value) for the all number of simulation runs and this is because the high number of malicious which we set at M=35.

The miss detection probability is averaged at 0.187 for the whole 600 runs, as one can see in Fig. 8.

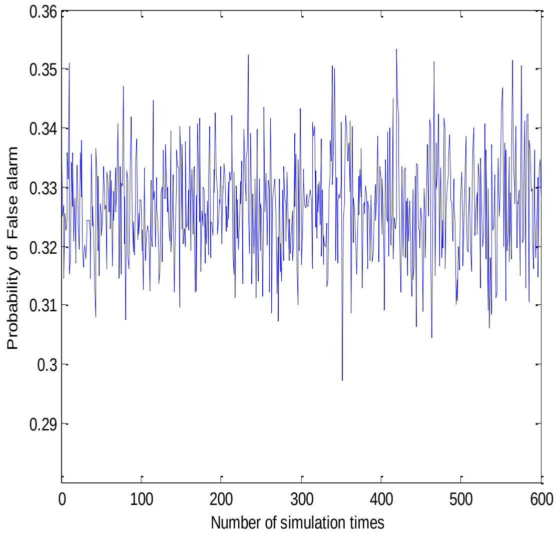

Figure 7. Probability of succefull PUEA (False e Alarm)

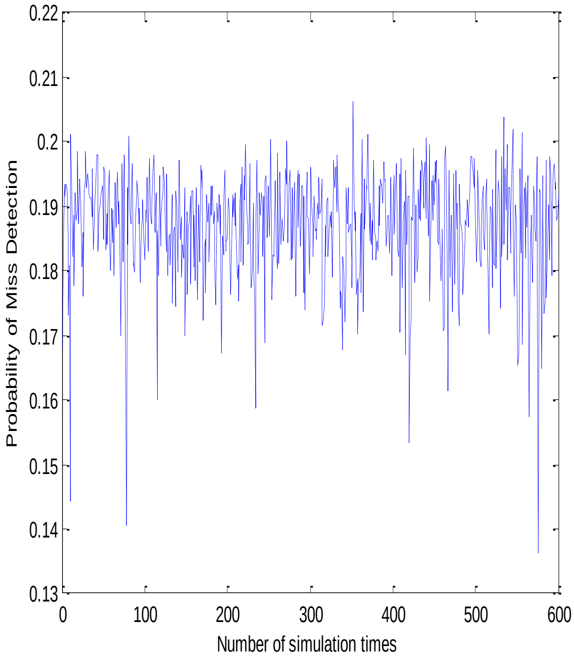

Figure 8. Probability of miss detection

We have done the simulation with different values of λ, as shown in Table III, and we have noted that when λ is decreased, the probability of successful PUEA decreased and the miss detection probability is increased; this is as expected, since NPCHT only allows a threshold to be set on either false alarm or miss detection probabilities.

TABLE III. FALSE ALARM AND MISS DETECTION FOR DIFFERENT VALUES OF λ

Parameter	False Alarm Probability Averaged for 600 runs	Miss Detection Probability Averaged for 600 runs
λ =2	0.326	0.187
λ =1	0.043	0.4182
λ =0.5	0.041	0.43

Finally, we have used the Cumulative Distribution Function (CDF) to describe and show how both the false alarms and miss detection probability appears on the same graph.

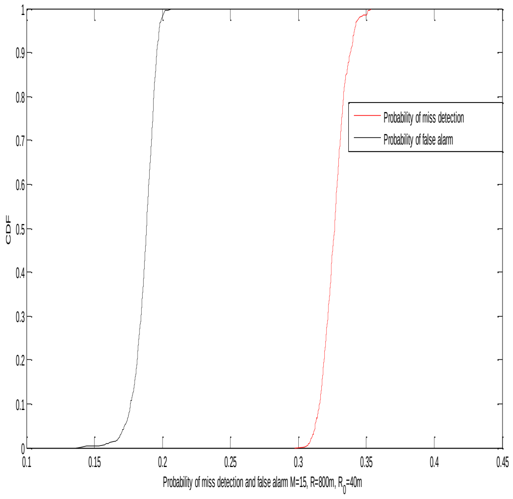

Figure 9. CDF of false alarm and miss detection probabilities

It is clear from Fig. 9 that the CDF plot is non-decreasing and right-continues function as must be meaning that the parameters and assumptions we have taken in our simulation are well-chosen and very close to the real-life values.

V. CONCLUSION AND FUTURE WORK

In this paper, we presented an analytical and experimental approach to obtain the PDFs of received powers at the secondary users due from malicious users and also due from the primary transmitter in a CR network by a set of malicious users.

The PDF obtained was used in Neyman-Pearson Composite Hypothesis Test to show the probability of false alarm in the network. Our results show that number of malicious users in the system has a great impact on the network causing the secondary users to suffer degradation in the quality of their communication due to the transmission from the malicious users. Also we show that there is a range of network radii in which PUEA are most successful.

The future work will be as a second stage of this work; in this stage, we will propose a security algorithm for transmitter verification scheme based on two parameters (distance and received signal power level) in order to identify the primary and malicious users; this kind of mitigation technique for PUEA does not rely on examination of PDF, but rather on localization of signal source.

ACKNOWLEDGMENT

As a research group, we are very thankful to Nick Riley and Kevin S. Paulson in Department of Engineering for their feedback and contributions in this work.

REFERENCES

[1] M. Buddhikot and K. Ryan, “Spectrum management in coordinated dynamic spectrum access,” IEEE DySpan, pp. 299–307, August 2005.

[2] FCC 03-322, “NPRM - Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing CR Technologies,” FCC, December 2003.

[3] Z. Jin, S. Anand, and K. Subbalakshmi, “Detecting primary user emulation attacks in dynamic spectrum access networks,” IEEE International Conference on Communications, Dresden, Germany, no. 4, pp. 13‑18, June 2009.

[4] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/CR wireless networks: A survey,” (Elsevier Journal), on computer Networks, vol. 50, no. 13, pp. 2127-2159, September 2006.

[5] Z. Kun, P. Paweczak, and D. Cabric, ”Reputation-based cooperative spectrum sensing with trusted nodes assistance,” IEEE Communications Letters, vol. 14, no. 3, pp.226-228, March 2010.

[6] T. Yucek, H. Arslan, ”A survey of spectrum sensing algorithms for CR applications,” IEEE Commun. Surveys Tutorials, vol.11, no.1, pp.116-130, First Quarter 2009.

[7] M. Kuroda, R. Nomura, and W. Trappe, ”A Radio-independent Authentication Protocol (EAP-CRP) for Networks of CRs,” 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, (SECON 2007), pp.70-79, 18-21, San Diego, California, USA, June 2007.

[8] D. Borth, R. Ekl, B. Oberlies, and S. Overby, ”Considerations for Successful CR Systems in US TV White Space,” in 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DySPAN 2008), pp. 1-5, 14-17 October 2008.

[9] R. Chen and J. Park, “Ensuring trustworthy spectrum sensing in CR networks,” Proceedings, IEEE Workshop on Networking Technol. for Software Defined Radio Networks (SDR), pp. 110–119, September 2006.

[10] R. Chen, J. M. Park, and J. H. Reed, “Defense against primary user emulation attacks in CR networks,” IEEE Journal on Selected Areas in Communications: Special Issue on CR Theory and Applications, vol. 26, no. 1, pp. 25–37, January 2008.

[11] S. Anand, Z. Jin, and K. P. Subbalakshmi, “An analytical model for primary user emulation attacks in CR networks,” Proceedings, IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks, pp. 35-40, October 2008.

[12] C. N. Mathur and K. P. Subbalakshmi, “Security issues in CR networks,” Chapter: Cognitive Networks: Towards Self-Aware Networks, John Wiley & Sons, Ltd, pp. 271–291, October 2007.

[13] G. Jakimoski and K. P. Subbalakshmi, “Denial-of-service attacks on dynamic spectrum access networks,” IEEE CogNets Workshop, IEEE International Conference on Communications (ICC) 2008, pp. 125-132, May 2008.

[14] S. Bhattacharjeea, S. Senguptab, and M. Chatterjee, ’’Vulnerabilities in CR networks’’ , The International Journal for the Computer and Telecommunications , Vol. 36, pp. 1387-1398 , October 2013.

[15] A. N. Mody, R. Reddy, T. Kiernan, and T.X. Brown, ”Security in CR networks: An example using the commercial IEEE 802.22 standard,” in IEEE Military Communications

Conference (MILCOM 2009), pp. 1-7, 18-21, Boston, MA, USA, 21 October 2009.

[16] N. R. Prasad, ”Secure Cognitive Networks,” in European Conference on Wireless Technology (EuWiT 2008), pp.107-110, 27-28 , Amsterdam, The Netherlands, October 2008.

[17] Z. Jin, S. Anand, and K. P. Subbalakshmi, “Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks,” in IEEE Transactions on Communications, vol. 60, no. 9, pp. 2635-2643, December 2012.

[18] Z. Jin, S. Anand, and K.P. Subbalakshmi, “Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing, ACM SIGMOBILE Mob. Comput. Commun. 13 (2), pp. 74–85, November 2009.

[19] T. S. Rappaport, “Wireless communications: principles and practice,” Prentice Hall Inc., New Jersey, June 1996.

[20] S. Anand, Z. Jin, and K. P. Subbalakshmi, “An Analytical Model for Primary User Emulation Attacks in CR Networks”, Proceedings, IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks, July 2008.

[21] E. Orumwense, O. Oyerinde, and S. neney, ’’Impact of Primary User Emulation Attacks on CR Networks’’, International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), vol. 4, no. 1, ISSN 2039 – 5086 February 2014.

Evaluation of Deterministic Medium Access Based on a Cooperative Cognitive Radio Approach

Yashar Naderpour, Dimitri Block, Uwe Meier
inIT - Institute of Industrial Information Technologies
Ostwestfalen-Lippe University of Applied Sciences
Lemgo, Germany
e-mail: {yashar.naderpour, dimitri.block, uwe.meier}@hs-owl.de

Abstract — **Caused by increasing demands for wireless devices in the last decade, license-free bands such as the 2.4 GHz ISM band become more and more crowded. As a consequence, interferences are inevitable. To avoid impairments caused by interferences, there have to be mechanisms to prevent coexisting systems to interfere with each other in license-free bands. Especially in industrial application fields, a reliable and deterministic medium access is required. In this paper, we evaluate an inter-system cooperation approach, which is designed to be aware of interferences, to ensure reliable real-time communication and further to protect investment for existing wireless systems. In a selected industrial scenario, it outperforms a non-cooperative approach especially in presence of interference. Further, it ensures a reliable communication for more than 99% of the real-time data packet transmissions also in presence of interference.**

Keywords - cognitive radio; control channel; deterministic medium access; inter-system automatic configuration

I. INTRODUCTION

*Cognitive radio (CR), "*firstly introduced by Joseph Mitola in 1999, is an emerging concept in the world of wireless communication" [1]. CR system is aware of its radio environment and therefore, detects interfering radio devices, which are called primary users (PUs). CR also identifies temporal and spectral opportunities for secondary user (SU) utilization. However, such prediction-based opportunity identification are prone to errors. Therefore, providing a deterministic medium access approach, which is able to be aware of its radio environment and to manage spectrum efficiency is highly desirable for CRs.

These solutions are also enablers for new industrial automation (IA) applications. IA applications require deterministic wireless medium access for reliable operation in real-time applications. As many wireless technologies – also for IA applications – share the same wireless channels such as the 2.4 GHz ISM band, a proper coexistence behavior is a fundamental requirement.

In this work, a proposed cooperative CR approach [2] is implemented and evaluated, which is called inter-system automatic configuration (ISAC). To the best of our knowledge, the proposed approach has not been implemented or evaluated yet.

ISAC's design has mainly three goals:

a) Interference awareness

b) Ensuring real-time and reliable communication

c) Investment protection for existing wireless systems

The first goal is necessary for IA applications to provide the second goal, real-time performance and reliable communications. ISAC systems aim to avoid interference with other wireless systems and protect themselves from being interfered.

The third goal focuses on implementation requirements. The ISAC approach unifies the spectrum utilization management. It is suitable for being integrated into existing industrial wireless solutions such as industrial WLAN, Bluetooth, WirelessHART, ISA100.11A, and ZigBee. The integration of the approach shall be therefore simple with minor protocol adaption.

This paper is organized as follows: Section II summarizes fundamentals about medium access and control channel usage. Section III illustrates the ISAC approach. Section IV specifies a selected measurement scenario, which is used for experimental evaluation. Section V analyses the results, and discusses the outcome. Finally, Section VI provides a conclusion for this paper.

II. STATE OF THE ART

IA applications provide harsh requirements for medium access methods (MAMs). To fulfill the requirements a cooperative approach among the users sharing the same environment with a proper controlling is necessary. A control channel (CC) is mandatory for this approach. In this section, the key issues MAMs and CCs are discussed in more detail.

A. Medium Access Methods

Multiple wireless devices utilize shared spectral, temporal, spatial resources. Therefore, wireless MAMs are approaching the issue of coexistence in different ways. They can be categorized into non-adaptive MAMs, adaptive MAMs, and cognitive MAMs [2][3]. They are briefly described in the following subsections.

1) *Non-Adaptive Medium Access Methods*

Non-adaptive MAMs use for example time-, frequency-, and code-division multiple-access (TDMA, FDMA, CDMA) [4]. They do not include any mechanism to mitigate interference and rely on central planning by a dedicated device or manual configuration. Due to their synchronous structure, non-adaptive MAMs require only a little communication overhead. Radio systems based on these MAMs provide a deterministic medium access in case of no interference. They are not aware of interference and therefore, show a poor coexistence behavior.

2) *Adaptive Medium Access Methods*

While non-adaptive MAMs show poor coexistence behavior, adaptive MAMs are aware of the radio environment. They are aware of the radio environment to a certain degree to improve the performance. Examples of such methods are carrier sense multiple access with collision avoidance (CSMA/CA) [4], ALOHA [5], and adaptive frequency hopping (AFH) [6].

Adaptive MAMs mitigate interference with others in order to approach error-free transmissions. On the other hand they have no deterministic behavior. Thus, adaptive MAMs require a communication overhead and additional synchronization effort. Adaptive MAMs can be distinguished with respect to the feedback instant of time: Listen-before-talk (LBT) [4] and listen after talk (LAT) [4]. LBT requires feedback before transmission. Such a medium access mechanism is CSMA/CA. If no new interference appears during transmission, LBT MAMs will ensure an error-free transmission.

In contrast to LBT MAMs, LAT MAMs react on a feedback instant of time after packet transmission. Typically, they are based upon service degradation such as packet reception failure. An example is Bluetooth AFH. After some packet loss in a certain frequency channel, it will be avoided for further packet transmissions by channel blacklisting for a specific time duration. Because LAT MAMs react after packet transmission, they cannot guarantee error-free transmissions.

3) *Cognitive Medium Access Methods*

Adaptive MAMs have a reactive nature. In contrast, cognitive MAMs are based on proactive approaches. They try to model the radio environment and adapt the wireless communication accordingly in order to improve the transmission performance and increase the spectrum efficiency. They can be classified into autonomous and cooperative approaches.

Autonomous CR systems improve the performance of a single radio system opportunistically. While, cooperative systems negotiate the resource allocation and optimize the performance of several systems in a certain environment. This negotiation requires a communication opportunity, which can be achieved via a control channel (CC).

B. *Control Channel*

The CR needs to sense the spectrum and select an appropriate channel for the SU communication. To achieve this, cooperative CRs communicate with each other via a CC [1]. Basically, the CC is a logical channel. Its implementation offers two possibilities:

1) Common control channel: The control messages are being exchanged on the same channel as used for the wireless solutions but during idle data phases. This solution is easy from a hardware point of view but requires a sophisticated time scheduling, which might conflict with desired real-time application.

2) Dedicated control channel: A separate physical channel is reserved for the exchange of control messages. Depending on the available hardware structure, the dedicated CC might use the same transceiver unit as the data messages. As mentioned before, the same sophisticated time scheduling is necessary. If two transceiver units for the data and control messages are available, the time scheduling is drastically simplified.

A separate transceiver unit might also support a wired CC if the application tolerates it. Further examples are given in [7].

III. Inter-System Automatic Configuration

The cooperative ISAC concept was published in [2] as work in progress. This paper contributes ISAC's implementation aspects, its evaluation and comparison with other approaches. The ISAC network consist of two different entities: ISAC supervisor and ISAC client. The ISAC network requires a single central ISAC supervisor and permits multiple ISAC clients. The ISAC supervisor uses the CC for communication.

A. *Supervisor*

The most important entity in an ISAC network is the ISAC supervisors for resource management.

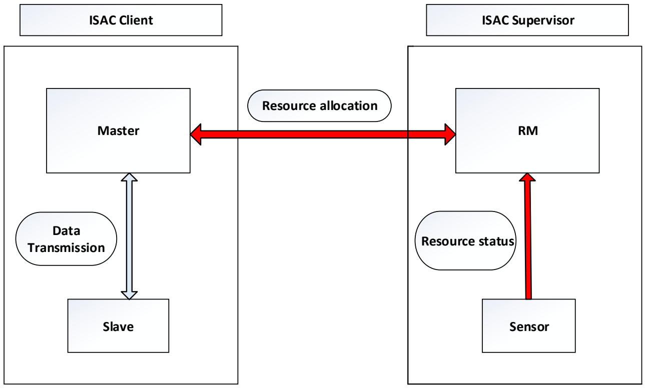

Figure 1. Basic ISAC network consist of ISAC supervisor and ISAC client connected via control channel (red arrows)

Thereby, the term resources refers to the hyperspace introduced in [8] consisting of multiple dimensions such as spectrum, time, code and the spatial dimension. The tasks of the ISAC supervisor are (i) resource allocation and (ii) interference mitigation. Therefore, it is equipped with the CR features of resource sensing and resource occupancy prediction.

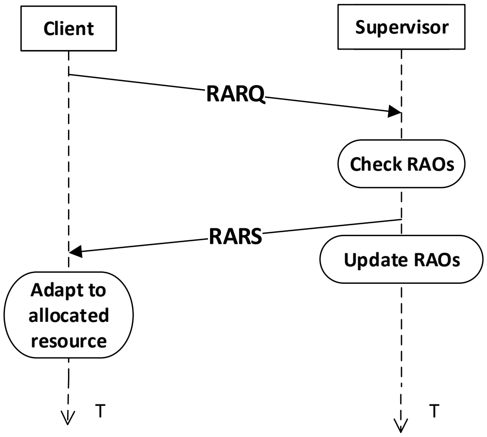

Figure 2. Sequence diagram of resource allocation negotiation between ISAC client and ISAC supervisor

As shown in Figure 1, the ISAC supervisor consists of two different wireless devices: Resource sensing device (sensor) and resource management device (RM). The sensor is

ISBN: 978-1-61208-403-9

responsible for resource sensing and predicting future behavior. Figure 2 shows the resource allocation negotiation procedure for two client. In case an ISAC client requests a resource allocation (RARQ), the RM selects the optimal resource allocation opportunity (RAO) according to the resource utilization capabilities of the ISAC client. Next, the RM response with the allocated resources (RARS) and the ISAC client tunes accordingly.

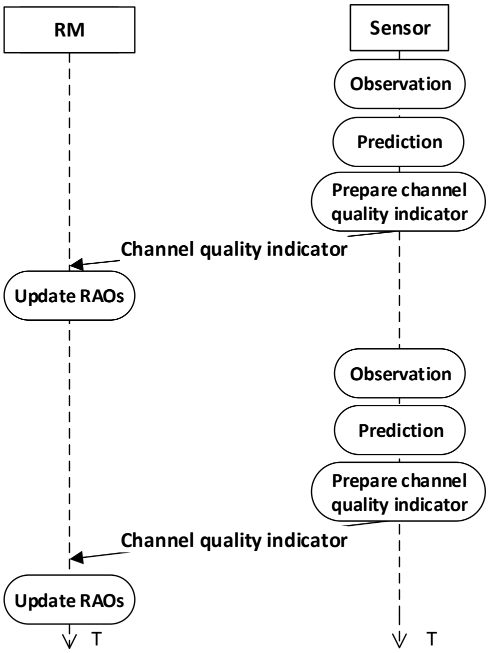
RM
Sensor
Observation
Prediction
Prepare channel quality indicator
Channel quality indicator
Update RAOs
Observation
Prediction
Prepare channel quality indicator
Channel quality indicator
Update RAOs
T
T

Figure 3. Sequence diagram of cyclic resource status reporting from sensor to resource manager

Additionally to resource allocation, the ISAC supervisor has to mitigate interferences, which could be either observed by the ISAC client or the ISAC supervisor's sensor. The sensor informs the RM about the resources status based on the resource sensing and prediction outcome. Then, the RM determines RAOs as illustrated in Figure 3. In case an ISAC client detects an interference within its utilized resources, it initiates a resource allocation negotiation within the limited resource utilization capabilities.

B. *Client*

The ISAC clients are resource users. The ISAC clients are independent wireless systems. In IA such wireless systems are Bluetooth piconets, WirelessHART mesh networks, or WLAN infrastructure networks. These wireless systems are used already for multiple applications like controlling or monitoring tasks. Each ISAC client has to provide a communication interface to the central ISAC supervisor. Typically, a good choice for the integration is the central management device of the certain wireless system like Bluetooth master, WirelessHART gateway, or WLAN access point, respectively.

The ISAC client's tasks are to (i) request for resource allocations from the ISAC supervisor and tune accordingly, and optionally to (ii) inform the ISAC supervisor about interferences. In order to reach the first task, the only mandatory requirement for the ISAC clients is to have tuning capabilities.

In order to reach the optional second task, the ISAC clients have to be equipped with sensing capabilities either listen-before-talk features such as WLAN and WirelessHART CSMA/CA or packet loss notification features. The sensing outcome can be used to initiate a resource allocation negotiation as mentioned above.

C. *Control Channel*

The ISAC CC is used for the communication between the ISAC supervisor and ISAC clients, and within the ISAC supervisor between RM and sensor. Further, the ISAC concept requires a dedicated CC, which has to be always available for communication. So, it has to be guaranteed that the CC never gets interfered by some PUs, SUs or any other kind of interferences.

IV. IMPLEMENTATION

The introduced general ISAC concept is implemented and evaluated within an IA scenario. The specific ISAC network setup is shown in Figure 4.

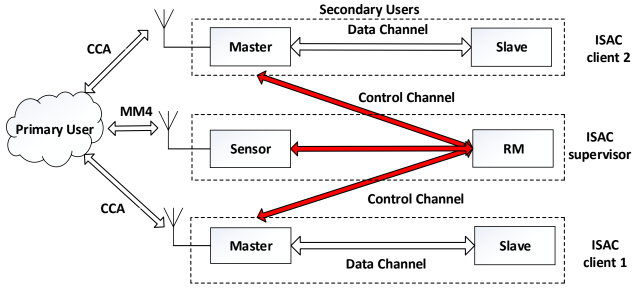

Figure 4. Measurement setup with interfering PU and SU containing an ISAC network with two ISAC clients

The master uses a frequency channel called data channel (DC) for data transmissions to its slave. Three frequency channels are available for data transmission. These three channels are named CH1, CH2, and CH3. These are the available spectral resources. Hence, the implementation is limited to spectral resources and does not consider the management of other resources such as temporal, code or spatial resources.

Another type of frequency channel is the dedicated CC, which is named CH0. For simplicity reasons, we assume that CH0 is not interfered by any primary user. In the following sections the SU and PU setups are discussed.

A. *Secondary User Setup: ISAC Clients*

In order to address a crowded IA scenario, we evaluate the ISAC network with two ISAC clients. Both ISAC clients are independent wireless systems performing real-time data transmission tasks. In order to lower the network implementation complexity, both ISAC clients are operating identically in a master-slave constellation, which is common in IA scenarios.

The master and slave are implemented in the microcontroller MSP430 of Texas Instruments (TI) with the narrowband transceiver CC2500. The master transmits data packets of fixed size and content while the slave returns the received data packets to acknowledge the correct reception. Important features and selected time parameters are summarized in Table I.

TABLE I: SU ISAC CLIENT MASTER AND SLAVE TEST-BED FEATURES

Platform	µC MSP430 with transceiver CC2500			
Channel	CH0	CH1	CH2	CH3
Center frequency	2.43 GHz	2.44 GHz	2.45 GHz	2.46 GHz
Channel Type	CC	DC	DC	DC
Spectrum sensing	No	RSSI-based CCA prediction		
Sample time	-	~ 90 µs		
Traffic	RARQ	Real-time data transmission		
Type	Event-based	Cyclic		
Period	-	40 ms		
Acknowledgment	-	Data echo		
QoS	No	PLR in %		
Packet duration	~1.2 ms	~2.7 ms		
Switching time	~ 100 µs			
Bit error detection	CRC-16			

Each ISAC client starts communication on the default DC. The master is equipped with the sensing feature listen-before-talk by a clear channel assessment (CCA) based on the received signal strength indication (RSSI) within its current DC. In case of successful CCA the data transmission is continued in the current DC. Otherwise the current DC is interfered by the PU or the other ISAC client. As shown in Figure 5, before next data transmission, the master tunes to the CC in order to initiate a resource allocation negotiation. The ISAC supervisor response with the new allocated DC. After receiving the response from ISAC supervisor, the master tunes to the previous DC in order to notify the slave about the new allocated DC. The master tunes to the new allocated DC, when the slave successfully acknowledges (ACK) the notification. In case the notification is unsuccessfully acknowledged from slave, the master continues sending notification till receiving successful acknowledged from slave.

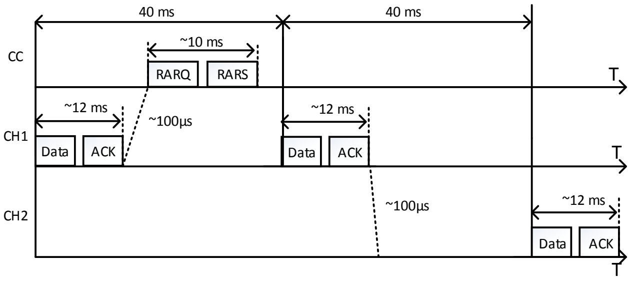

Figure 5. Timing diagram of master-slave resource allocation change within real-time data communication

The master does not stop data transmission during resource allocation negotiation. In case of resource allocation negotiation between master and supervisor failure, the master will tune to previous DC and will try to continue data transmission. With the next CCA failure, the master initiates a new resource allocation negotiation with ISAC supervisor. Therefore, the master does not lose any data transmission. The master performs the CC communication within its idle time. As a consequence, data transmission is always in real-time.

B. Secondary User Setup: ISAC Supervisor

The ISAC supervisor contains the sensor and the RM specified in Table II and Table III, respectively. The sensor and RM are also implemented in the microcontroller TI MSP430 with the narrowband transceiver TI CC2500.

TABLE II: SU ISAC SUPERVISOR SENSOR TEST-BED FEATURES

Platform	µC MSP430 with transceiver CC2500
Channel type	CC
Center frequency	2.43 GHz
Data packet duration	~1.2 ms
Bit error detection	CRC-16
Spectrum sensing	MM4-based DCs occupancy prediction
Acknowledgment	No
Traffic type	Cyclic
Idle time	30 ms
Duty cycle	~4 %
Period	~31.2 ms

The sensor senses all DCs periodically. Then, it determines two measures derived from the Markov model MM4 published in [2][9]. The first measure is the busy distance expressing the observed mean count of consecutive occupied samples within a certain DC, which are interfered by PUs. The second measure is the idle distance expressing the mean count of consecutive non-occupied samples, respectively. Based on the difference between the busy and idle distances, the DCs are sorted according to their quality. This information is given to the RM as DC quality indicators. Hence, the DC quality indicators provide information about the amount of interference of each DC.

TABLE III: SU ISAC SUPERVISOR RESOURCE MANAGER TEST-BED FEATURES

Platform	µC MSP430 with transceiver CC2500
Channel type	CC
Center frequency	2.43 GHz
Data packet duration	~1.2 ms
Bit error detection	CRC-16
Traffic	RARS
Type	Event-based

The RM has the responsibility to update the RAO. Therefore, it stores the very last DC quality indicators permanently. Hence, upcoming resource allocation decisions are based on the last stored DC quality indicators.

C. Primary User Setup

TABLE IV: PU TEST-BED FEATURES

Platform	Vector Signal Generator SMBV100A
PU type	Cyclic IEEE 802.11g-like transmission
Center frequency	2.45 GHz
Data packet duration	~2 ms
TX power	15 dBm
Traffic type	Cyclic
Idle time	10 ms
Duty cycle	~16.7 %
Period	~12 ms

A selected PU activity is based upon IEEE 802.11g-like transmissions, which is common in IA scenarios. The PU activity is generated by a vector signal generator. Further important features and selected time parameters for the PU are summarized in Table IV. While the SUs are sensitive to the radio environment, the PU performs cyclic data transmission without feedback from the radio environment based on CSMA/CA. The PU is a single device, which transmits data packets with a duration of 2 ms and a period of 12 ms. It is important to note, that only CH2 is interfered by the PU.

V. Result and Analysis

In this section, we present the ISAC results in comparison to an appropriate reference.

A. Implementation Validation

The cyclic SU and PU emissions using ISAC are illustrated in the measured spectrograms in Figure 6 and Figure 7. The measurements were done with the real-time spectrum analyzer Tektronix RSA6114A. The horizontal and vertical axis represent the frequency and the time, respectively. CH0 is CC and CH1, CH2 and CH3 are the defined DCs.

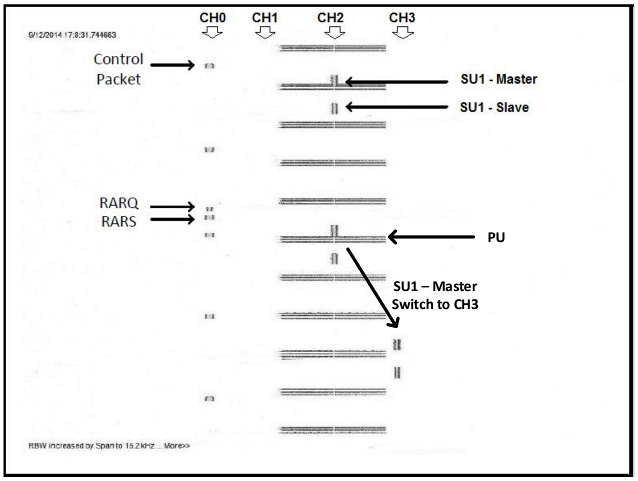

Figure 6. Spectrogram of the resource allocation negotiation with RARQ and RARS within the control channel of SU master and slave to avoid PU interference

The spectrogram ranges from 2.43 GHz to 2.48 GHz and has a duration of 100 ms.

Figure 6 shows the cyclic operation of the PU interfering CH2 where an ISAC client is transmitting data. This PU activity causes packet loss. The ISAC client detects PU activity and sends a RARQ to the RM. Then, according to RARS from the RM, the ISAC client tunes to the allocated free DC and therefore, bypasses future activity of the PU.In case of multiple ISAC clients, the RM allocates different DCs to each ISAC client while observing the PU interference.

As shown by the example in Figure 7, the PU interferes CH2 only while the ISAC clients transmit data in CH1 and CH3.

B. Experimental Results

For evaluation, we measured the QoS within two different scenarios, which differ in the presence of PU interference. Within each scenario, we performed experiments for three different medium access types: Non-sensing (NS), non-cooperative (NC), and ISAC-based medium access. The implementation of the latter one was introduced in Section IV.

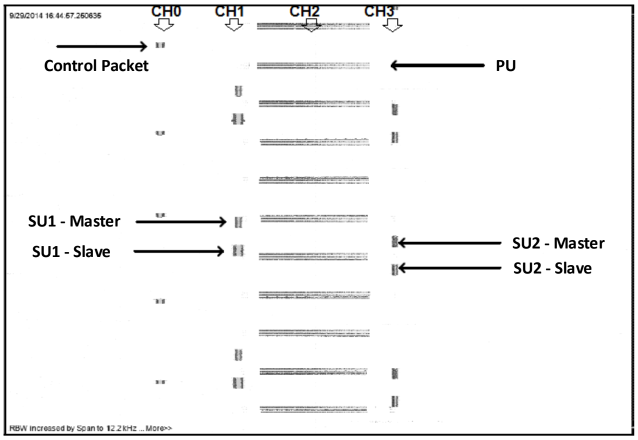

Figure 7. Spectrogram of two SU master-slave data transmissions within different frequency channels allocated by the resource manager

The NC medium access neglects the usage of the cooperative ISAC concept. I.e. each SU client works independently. In this setup, the master performs a CCA based on MM4 before each data transmission in the default DC CH2 as published in [2][9]. In case of CCA failure, the master switches to the backup DC CH3 after informing the slave. Hence, they try to omit the backup DC as much as possible.

The NS medium access even reduces the complexity of the non-cooperative medium access. The master does not sense the spectrum in terms of any CCA. Therefore, it is not able to predict spectrum occupancy or to detect PU interference. The master does not tune to any other channel either. Hence, there will be data transmission collisions and packet loss. The experiments are performed with a measurement duration for 1000 data packet transmissions, which are repeated 5 times and are averaged to result in a representative evaluation. Thereby, the master of both real-time wireless systems for each experiment determines the packet loss rate (PLR) as a measure of QoS. For each failure in receiving the correct ACK, the master increase the number of packet losses. Figure 8 and Figure 9 show the result of all experiments in case of PU interference absence and presence, respectively. The horizontal and vertical axis represent the medium access types in different devices and the PLR, respectively in Figure 8 and Figure 9.

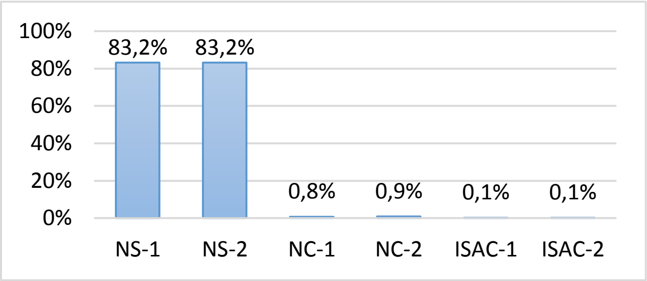

Figure 8. PLR (vertical axis) of two master-slave constellations (index 1 and 2) for the medium access methods (horizontal axis) non-sensing (NS), non-cooperative (NC) and ISAC in absence of PU

They show the PLRs for both real-time wireless systems. Clearly, NS medium access has the worst performance in both scenarios. This results from its non-cooperative and non-adaptive medium access. In case of no PU interference, the two real-time wireless systems interfere each other.

The same disturbance can be observed also for the NC medium access but the PLR is below one percent without PU activity. The NC medium access avoids the PU interference much better than the NS medium access. However, the PLR is above 25% with PU activity.

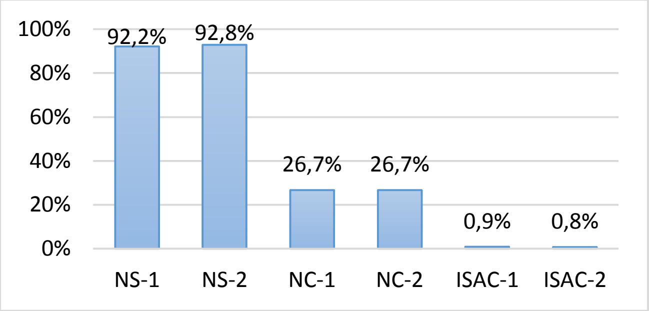

Figure 9. PLR (vertical axis) of two master-slave constellations (index 1 and 2) for the medium access methods (horizontal axis) non-sensing (NS), non-cooperative (NC) and ISAC in presence of PU

The best performance can be seen for the ISAC-based medium access. The PLR is below one percent even in presence of PU interference.

VI. Conclusion and Future Work

The paper introduces a cooperative cognitive radio approach implementation providing a deterministic medium access called inter-system automatic configuration approach (ISAC). Its performance is evaluated to face the increasing demands for industrial wireless devices in license-free bands. ISAC focuses on the industrial automation requirements of (i) interference awareness, (ii) ensuring real-time and reliable communication, and (iii) investment protection for existing wireless systems.

A central radio device manages the allocation of resources such as frequency channels, time slots and spatial resources in a cooperative inter-system manner to ensure reliable communication. Further, a sensing radio device reports the resource status continuously for awareness of non-cooperative wireless systems and other interferences in the radio environment. Additionally, each cooperative wireless system has to negotiate resource allocations and to notify interferences. Therefore, a single device has to be replaced or updated with an appropriate communication interface and configuration with adaption capabilities. This minor modification of existing wireless systems ensures investment protection. It is important to note that ISAC's central radio device communication is performed in a dedicated control channel.

The evaluations are done for a selected industrial scenario in a test-bed based on multiple radio devices with TI MSP430 microcontroller and TI CC2500 narrowband transceiver. Two industrial wireless systems with a real-time master-slave constellation are deployed and act as secondary users. They cooperate via the control channel with the central resource manager radio device. Thereby, three different frequency channels serve as resource opportunities, which are partly interfered by a non-cooperative primary user. The primary user represents an infrastructure-based IEEE 802.11 wireless system often applied in factory automation. The interferences are sensed and reported via a control channel in terms of frequency channel occupancy prediction with an additional radio device.

To show the benefits of cooperation, ISAC's performance is compared with a (i) non-cooperative and with a (ii) non-cooperative non-sensing approach, which are also introduced and explained in detail. Thereby, ISAC outperforms both approaches especially in the presence of primary user interference. Hence, cooperation increases interference awareness significantly. Further, ISAC ensures a reliable communication for more than 99% of the real-time data packet transmissions independently of primary user interference presence. Hence, reliable communication can be ensured.

Further investigations shall advance the resource allocation to multiple dimensions such as time and spatial resources. Additionally, hybrid allocation schemes mixing central and distributed decision-making may be evaluated to lower latency especially for temporal resource allocation without losing the benefits of central management. Also, the evaluation of a common control channel may be investigated, which shares the same licensed-free band for convenience reasons and further investment protection.

Acknowledgment

This paper is based on the research project 17041X11 of the German Federal Ministry of Education and Research (BMBF).

References

[1] E. Hossain and V. K. Bhargava, “Cognitve Wireless Communication Network” in Springer, Vancouver, Canada, 2007.

[2] D. Block and U. Meier, “Wireless Deterministic Medium Access: A Novel Concept Using Cognitive Radio”. The Third International Conference on Advances in Cognitive Radio - COCORA 2013, Apr 2013, pp 35-38.

[3] D. Block, Y. Naderpour, G. M. Shrestha, and U. Meier, “Performance Evaluation of Cognitive Wireless Medium Access Method in Industrial Coexisting Environment”, Emerging Technologies & Factory Automation (ETFA), 2012 IEEE 17th Conference on, vol., no., Sept.2013, pp 30-34.

[4] T. S. Rappaport, “Wireless communication,” New Jerssey, USA, Prentice Hall, 2002.

[5] N. Abramson, “The ALOHA System: Another Alternative for Computer Communications,” in Proceedings of the Nov 17-19, 1970, fall joint computer conference. ACM, 1970, pp. 281–285.

[6] “Bluetooth Core Specification v1.2,” 2003.

[7] J. Marinho and E. Monteiro, “Cognitive Radio: Survey on Communication Protocols, Spectrum Decision Issues, and Future Research Directions”, Springer science business media LLC, 2011, New York, USA,.

[8] K. Ahmad, P. Ostfeld, U. Meier, and H. Kwaśnicka, “Exploitation of Multiple Hyperspace Dimensions to Realize Coexistence Optimized Wireless Automation Systems”, Industrial Informatics, IEEE Transactions on , vol.6, no.4, Nov. 2014, pp.758,766.

[9] K. Ahmad, U. Meier, and S. Witte, “Predictive opportunistic spectrum access using Markov models”, Emerging Technologies & Factory Automation (ETFA), 2012 IEEE 17th Conference on , vol., no., Sept. 2012, pp.1,10, 17-21.

Performance Analysis of Multi-Antenna Hybrid Detectors and Optimization with Noise Variance Estimation

Daniel Riviello, Pawan Dhakal and Roberto Garello
Department of Electronics and Telecommunications
Politecnico di Torino
Torino, Italy
Email: daniel.riviello@polito.it, pawan.dhakal@polito.it, garello@polito.it

Abstract—**In this paper, a performance analysis of multi-antenna spectrum sensing techniques is carried out. Both well known algorithms, such as Energy Detector (ED) and eigenvalue based detectors, and an eigenvector based algorithm, are considered. With the idea of auxiliary noise variance estimation, the performance analysis is extended to the hybrid approaches of the considered detectors. Moreover, optimization for Hybrid ED under constant estimation plus detection time is performed. Performance results are evaluated in terms of Receiver Operating Characteristic (ROC) curves and performance curves, i.e., detection probability as a function of the Signal-to-Noise Ratio (SNR). It is concluded that the eigenvector based detector and its hybrid approach are able to approach the optimal Neyman-Pearson performance.**

Keywords–hybrid detector; largest eigenvector; noise estimation; spectrum sensing; cognitive radio.

I. Introduction

Spectrum sensing is the enabling unit of Secondary Users (SUs) in Cognitive Radio Networks (CRN) [1] for the accurate identification and exploitation of unused Primary User's (PU) spectrum in temporal and spatial domain. Precise identification of the spectrum holes is the major constraint for the establishment of Cognitive Radio, which ensures the dynamic exploitation of existing wireless spectrum. As an example, the Wireless Regional Area Network (WRAN) standard imposes stringent requirement on the probability of detection $(P_d) \geq 0.9$ with probability of false alarm $P_{Fa} \leq 0.1$ at Signal-to-Noise Ratio (SNR) $-20dB$ (for Digital TV band) [3].

In order to satisfy the constraint of high performance and considering the dependence of noise uncertainty and the implementation complexity under wireless fading channels, several detection algorithms are put forward in context of Cognitive Radio applications including Uniformly Most Powerful (UMP) test derived according to the Neyman-Pearson Lemma known as Neyman-Pearson (NP) test [2], Energy Detection (ED) [4], Match Filtering [5], Feature Detection Algorithms [6] proposed for individual SU and their cooperative counterpart for multiple SU sensing. A multidimensional CR receiver has been studied considering multiple receive dimensions at the CR receiver in the form of multiple antennas, over-sampled branches and cooperative nodes [7]–[10]. These methods are mostly based on the statistics of the eigenvalues of the received signal covariance matrix and use recent results from Random Matrix Theory (RMT).

In the last few years, Eigenvalue Based Detection (EBD) techniques received considerable attention in spectrum sensing literature with improved performance and less dependent on noise uncertainty [7]–[16]. Some of the popular EBD based techniques in present literature include Maximum Eigenvalue (ME) based [14], Eigenvalue Ratio Detector (ERD) [17], Signal Condition Number (SCN) based [10][12], Scaled Largest Eigenvalue (SLE) based [15][16], Akaike Information Criterion (AIC) [18], Minimum Description Length(MDL) [18]. Recently, more powerful techniques based on largest eigenvalue of the received covariance matrix, like Generalized Likelihood Root Test (GLRT) [20] and Roy's Largest Root Test (RLRT) [19] have been proposed and analyzed. Recently, a new algorithm known as EigenVEctor (EVE) test [21] has been introduced exploiting channel estimation parameter in the detection statistic whose performance is comparable with NP test.

Considering high performance detection algorithms like ED, RLRT and EVE test, the problem of unknown noise variance is crucial. In our previous work [21][22], the performance of hybrid approach of ED and Roy's Largest Root Test using estimated noise variance was carried out. It was suggested that, the optimum performance of ED and RLRT can be achieved even with the use of estimated noise variance by using a large number of slots for noise variance estimation.

In this work, we present a performance analysis of Roy's Largest Root Test (RLRT), Energy Detection (ED), EigenVEctor Test (EVE) and their hybrid approaches with noise variance estimation. Section II describes the system model and the NP test, which will be used as a benchmark. Section III illustrates the test statistics with known noise variance, while Section IV presents the hybrid approaches with estimated noise variance. Simulation results are presented in Section V, while in Section VI, some preliminary results of the optimization of Hybrid Energy Detection are presented. Finally, Section VII concludes the paper.

II. System model

Let us denote by K the number of antennas or cooperative sensors and by N the number of samples per sensing slot. We focus on a single source scenario, which is of interest for many detection problems in cognitive radio networks. The $K \times 1$ received vector at time n collects the baseband complex samples from the K antennas. The received samples are stored by the detector in the $K \times N$ matrix $\boldsymbol{Y}$.

Let us introduce the $1 \times N$ signal matrix $\boldsymbol{s} \triangleq [s_1 \cdots s_n \cdots s_N]$ and the $K \times N$ noise matrix $\boldsymbol{V} \triangleq [\boldsymbol{v}_1 \cdots \boldsymbol{v}_n \cdots \boldsymbol{v}_N]$ where,

- s_n is the transmitted complex signal sample at time n, modeled as Gaussian with zero mean and variance $\sigma_s^2 : s_n \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_s^2)$

- $\boldsymbol{v}_n$ is a noise vector at time n, modeled as Gaussian with mean zero and variance σ_v^2 : $\boldsymbol{v}_n \sim \mathcal{N}_{\mathbb{C}}(\mathbf{0}_{K\times 1}, \sigma_v^2 \boldsymbol{I}_{K\times K})$

As all the signal samples s_n of $\boldsymbol{s}$ and the noise vectors $\boldsymbol{v}_n$ of $\boldsymbol{V}$ are assumed statistically independent, the detector must distinguish between Null and Alternate Hypothesis given by,

$$\boldsymbol{Y}|_{H_0} = \boldsymbol{V} \qquad \text{and} \qquad \boldsymbol{Y}|_{H_1} = \boldsymbol{hs} + \boldsymbol{V}$$

where, $\boldsymbol{h}$ is the complex channel vector $\boldsymbol{h} = [h_1 \cdots h_K]^T$; assumed to be constant and memory-less during the sampling window.

Under $\mathcal{H}_1$, the average SNR at the receiver is defined as, $\rho \triangleq \frac{\mathcal{E}\|\boldsymbol{x}_n\|^2}{\mathcal{E}\|\boldsymbol{v}_n\|^2} = \frac{\sigma_s^2\|\boldsymbol{h}\|^2}{K\sigma_v^2}$ where, $||.||$ denotes the Euclidean norm and $\mathcal{E}$ the mean operator. The sample covariance matrix is given by $\boldsymbol{R} \triangleq \frac{1}{N}\boldsymbol{Y}\boldsymbol{Y}^H$ and $\lambda_1 \geq \cdots \geq \lambda_K$ its eigenvalues sorted in decreasing order.

The usual criterion for comparing two tests is to fix the false alarm rate P_{fa} and look for the test achieving the higher P_d. The Neyman Pearson (NP) lemma is known to provide the Uniformly Most Powerful (UMP) test, achieving the maximum possible P_d for any given value of P_{fa}. The NP criterion is applicable only when both both $\mathcal{H}_0$ and $\mathcal{H}_1$ are simple hypotheses. In our setting this is the case when both the noise level σ_v^2 and the channel vector $\boldsymbol{h}$ are a priori known. The NP test is given by the following likelihood ratio:

$$T_{NP} = \frac{p_1(\boldsymbol{Y}; \boldsymbol{h}, \sigma_s^2, \sigma_v^2)}{p_1(\boldsymbol{Y}; \sigma_v^2)} \qquad (1)$$

and is known to be optimal, i.e., to achieve the maximum possible P_d for any given value of P_{fa}.

As an example, under the considered model, if the signal samples are independent Gaussian samples, the NP test is obtained by using:

$$\boldsymbol{p}_0(\boldsymbol{Y}; \sigma_v^2) = \frac{1}{(\pi\sigma_v^2)^{NK}} \exp\left(-\frac{N\boldsymbol{trR}}{\sigma_v^2}\right) \qquad (2)$$

and

$$p_1(\boldsymbol{Y}; \boldsymbol{h}, \sigma_s^2, \sigma_v^2) = \frac{1}{(\pi^K det\boldsymbol{\Sigma})^N} \exp\left(-\boldsymbol{R}\boldsymbol{\Sigma}^{-1}\right) \qquad (3)$$

where, $\boldsymbol{\Sigma} = \sigma_v^2 \mathbf{I}_k + \sigma_s^2 \boldsymbol{h}\boldsymbol{h}^H$

The NP test provides the best possible performance, but requires exact knowledge of both $\mathbf{h}$ and σ_v^2. For most practical applications, the knowledge of $\mathbf{h}$ and σ_v^2 is questionable.

III. Test statistics with known noise variance

To make the decision between $\mathcal{H}_0$ and $\mathcal{H}_1$, a test statistic compares a quantity T against a pre-defined threshold t: if $T > t$, $\mathcal{H}_1$ is selected, otherwise $\mathcal{H}_0$ is chosen. The test performance is evaluated by the false alarm probability and the detection probability, defined as:

$$P_d = \mathbb{P}(T > t|\mathcal{H}_1) \qquad (4)$$
$$P_{fa} = \mathbb{P}(T > t|\mathcal{H}_0) \qquad (5)$$

In practice, the decision threshold t is typically computed as a function of the target P_{fa}, to guarantee the Constant false Alarm rate (CFAR) property.

A. Roy's Largest Root Test (RLRT)

Using the information of the received signal matrix $\boldsymbol{Y}$ and assuming a perfect knowledge of the noise variance σ_v^2 and the channel parameter $\boldsymbol{h}$, test statistic for RLRT is given by

$$T_{RLRT} = \frac{\lambda_1}{\sigma_v^2}. \qquad (6)$$

If $T_{RLRT} < t$ it decides in favor of Null Hypothesis $\mathcal{H}_0$ otherwise in favor of Alternate Hypothesis $\mathcal{H}_1$. The detection probability $P_d^{RLRT} > t|_{\mathcal{H}_1}$ and false alarm $P_{fa}^{RLRT} > t|_{\mathcal{H}_0}$ probabilities for this detector are well-known in the literature (e.g., [24]).

The optimality of RLRT in the class of semi-blind algorithms was pointed out in [25]. For a single emitting source, if the SNR is above the identifiability threshold given by $\rho > \rho_{Cric} = \frac{1}{\sqrt{KN}}$ [26], the signal is detectable by the largest eigenvalue λ_1 value. Starting from the NP test and using the asymptotic expansion of the hypergeometric function, it was shown in that, under known noise variance, distinguishing between $\mathcal{H}_0$ and $\mathcal{H}_1$ in the asymptotic regime ($N \to \infty$ with K fixed) depends to leading order only on λ_1.

B. Energy Detection (ED)

ED computes the average energy of the received signal matrix $\boldsymbol{Y}$ normalized by the noise variance σ_v^2 and compares it against a predefined threshold t_{ed}.

$$T_{ED} = \frac{1}{KN\sigma_v^2} \sum_{k=1}^{K} \sum_{n=1}^{N} |y_k(n)|^2. \qquad (7)$$

If $T_{ED} < t_{ed}$ it decides in favor of Null Hypothesis $\mathcal{H}_0$ otherwise in favor of Alternate Hypothesis $\mathcal{H}_1$. The detection probability $P_d = Prob\{T_{ED} > t|_{H_1}\}$ and false alarm $P_{fa} = Prob\{T_{ED} > t|_{H_0}\}$ probabilities for this detector are well-known in the literature (e.g., [4]).

C. EigenVEctor Test (EVE)

The starting idea of the new test is that given a $\mathcal{H}_1$ slot, the eigenvector $\boldsymbol{e}_1$ associated to largest eigenvalue λ_1 provides an estimation of the channel vector $\boldsymbol{h}$.

Given S_{aux} signal slots available before the current sensing slot, we can construct a matrix of size $K \times (S_{aux} \cdot N)$ from all the samples and evaluate the eigenvector $\boldsymbol{e}_{aux}$ corresponding to largest eigenvalue. The proposed statistical test known as EVE test [10], which exploits the channel estimation parameter $\boldsymbol{e}_{aux}$ in its test statistic is defined as,

$$T_{EVE} = \frac{S_{aux}\left[\boldsymbol{e}_{aux}^H \boldsymbol{R}\, \boldsymbol{e}_{aux}\right] + \left[\boldsymbol{e}^H \boldsymbol{R}\, \boldsymbol{e}\right]}{\sigma_v^2 (S_{aux} + 1)} \qquad (8)$$

Note that if $S_{aux} = 0$, the test reduces to

$$T_{EVE} = \frac{\boldsymbol{e}^H \boldsymbol{R}\, \boldsymbol{e}}{\sigma_v^2} = \frac{\|\boldsymbol{e}\|^2 \lambda_1}{\sigma_v^2} = \frac{\lambda_1}{\sigma_v^2} \qquad (9)$$

and has the same statistical power of the RLRT.

IV. Hybrid test statistics

It is evident that the knowledge of the noise variance is imperative for the optimum performance of RLRT, ED and EVE tests. Unfortunately, the variation and the unpredictability of noise variance is unavoidable. Thus, the knowledge of the noise variance is one of the critical limitations of those tests for their ideal operation in low SNR. Under the considered scenario, noise variance can be estimated from S_{aux} auxiliary noise-only slots in which we are sure that the primary signal is absent.

Consider a sampling window of length M prior and adjacent to the detection window which contains noise-only samples for sure. Then the estimated noise variance from the noise-only samples using a Maximum Likelihood Estimation (MLE) can be written as,

$$\hat{\sigma}_v^2 = \frac{1}{KM}\sum_{k=1}^{K}\sum_{m=1}^{M}|v_{km}|^2 \tag{10}$$

If the noise variance is constant, the estimation can be averaged over S_{aux} successive noise-only slots and (10) can be modified by averaging over S_{aux} successive noise-only slots as,

$$\hat{\sigma}_v^2(S_{aux}) = \frac{1}{KS_{aux}M}\sum_{s=1}^{S_{aux}}\sum_{k=1}^{K}\sum_{m=1}^{M}|v_{km}|^2 \tag{11}$$

A. Hybrid RLRT (HRLRT)

Knowledge of the noise power is one of the critical limitation of RLRT for its operation in low SNR. Hybrid RLRT (HRLRT) [22] deals with the study of detection performance of the RLRT algorithm using noise variance estimated from S_{aux} auxiliary noise only slots where we are sure that the primary signal is absent. The test statistic of HRLRT can now be presented as,

$$T_{HRLRT} = \frac{\lambda_1}{\hat{\sigma}^2_{HRLRT}(S_{aux})} \tag{12}$$

where, $\hat{\sigma}^2_{HRLRT}(S_{aux})$ is the Maximum Likelihood Estimate of the true noise variance σ_v^2 given by (11).

Performance of HRLRT in terms of ROC parameters are derived and well justified in [22][23].

B. Hybrid ED (HED)

Hybrid ED (HED) [22] deals with the study of detection performance of the ED algorithm using noise variance estimated from S_{aux} auxiliary noise only slots where we are sure that the primary signal is absent. The test statistic of HED can be presented as,

$$T_{HED} = \frac{1}{KN\hat{\sigma}^2_{HED}(S_{aux})}\sum_{k=1}^{K}\sum_{n=1}^{N}|y_k(n)|^2 \tag{13}$$

where $\hat{\sigma}^2_{HED}(S_{aux})$ is computed as in (11) for HRLRT. The detection probability $P_d = Prob\{T_{HED} > t|_{H_1}\}$ and false alarm $P_{fa} = Prob\{T_{HED} > t|_{H_0}\}$ probabilities for this Hybrid ED can be referred in literature [22][23].

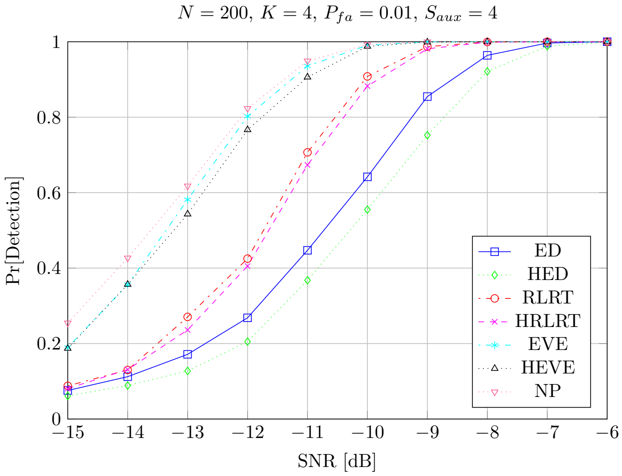

Figure 1. Performance curve, Pd vs. SNR, $K = 4$, $N = 200$

C. Hybrid EVE (HEVE)

If we apply the same hybrid approach for RLRT and ED of [22][23] to the new EVE test, we define a new Hybrid EigenVEctor (HEVE) test:

$$T_{HEVE} = \frac{S_{aux}\left[\boldsymbol{e}_{aux}^H\boldsymbol{R}\,\boldsymbol{e}_{aux}\right] + \left[\boldsymbol{e}^H\boldsymbol{R}\,\boldsymbol{e}\right]}{\hat{\sigma}^2_{HEVE}(S_{aux})\cdot(S_{aux}+1)} \tag{14}$$

where $\hat{\sigma}^2_{HEVE}(S_{aux})$ is computed as in (11) for HRLRT and HED. In fact, we use in HEVE the same number of slots S_{aux} both to compute the eigenvector $\boldsymbol{e}_{aux}$ for channel estimation and to estimate the noise variance $\hat{\sigma}^2_{HEVE}(S_{aux})$. Similarly to (9) if $S_{aux} = 0$, the test reduces to $\lambda_1/\hat{\sigma}^2_{HEVE}(S_{aux})$, which has the same statistical power of HRLRT.

V. Simulation results

Results are shown in terms of Receiver Operating Characteristic (ROC) curves (P_d vs. P_{fa}) and performance curves, in which P_d is plotted against SNR, by fixing P_{fa}. All the tests described in Section III-IV have been simulated by using a Montecarlo approach with 10000 iterations for each SNR value. The primary signal has a Gaussian distribution and the typical Rayleigh flat fading channel scenario has been considered. In performance curves, P_{fa} is fixed to 10^{-2} while in ROC curves, SNR = -12 dB.

Figures 1 and 2 show respectively the performance and ROC curves of all the test statistics with 4 antennas, 200 samples per slot and 4 auxiliary slots. It can be noticed that EVE and HEVE are clearly capable to significantly reduce the gap with NP wrt RLRT. The gap between EVE and RLRT is 1 dB at $P_d = 0.9$. In general, the hybrid approaches HEVE, HRLRT and HED are very close in performance with their respective known-noise tests.

Figures 3 and 4 show how the number of slots affects the performance of these tests. The number of antennas is equal to 4, while we used 200 samples per slot. It is evident that there is an important gap between 2 and 4 auxiliary slots (especially for HEVE), while the curves with 4 and 6 auxiliary slots are almost overlapped.

Finally, we show 2 other performance curves. In Figure 5, the detection probability is plotted against the number of

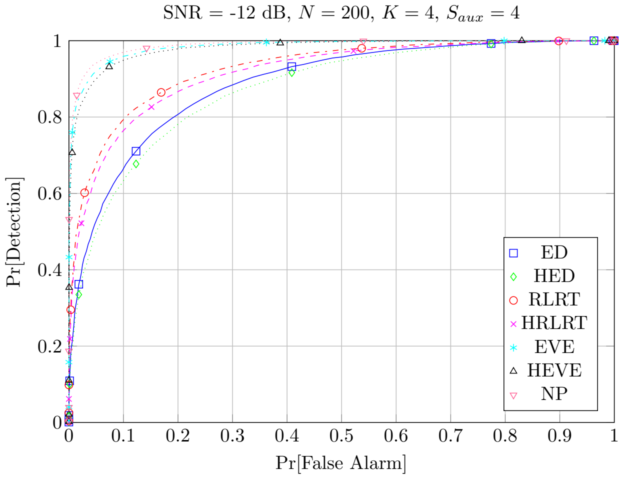

Figure 2. ROC curve, $K = 4$, $N = 200$

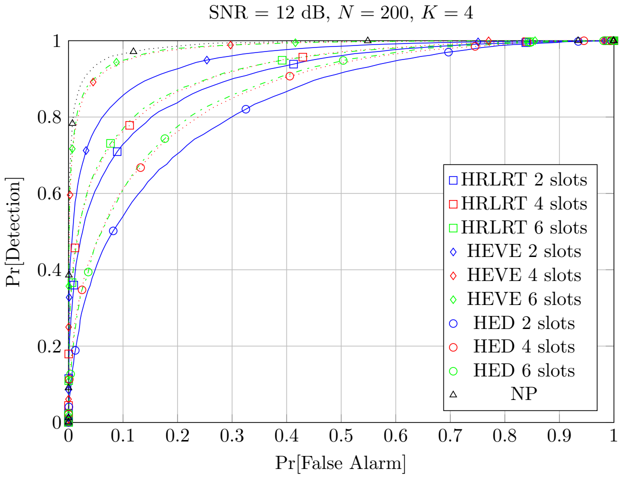

Figure 4. ROC curve, with 2, 4, 6 auxiliary slots

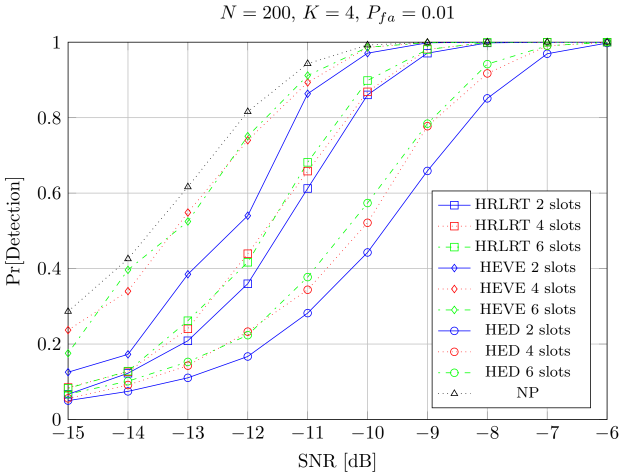

Figure 3. Performance curve, Pd vs. SNR, with 2, 4, 6 auxiliary slots

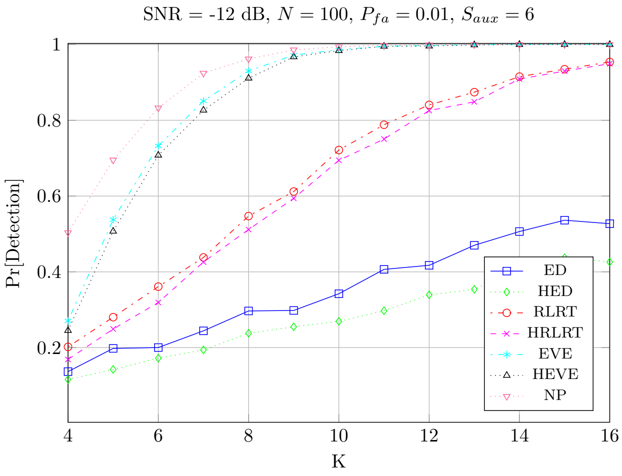

Figure 5. Performance curve, Pd vs. K, $N = 100$

antennas, with 100 samples per slot and 6 auxiliary slots, while in Figure 6, P_d is plotted against the number of samples, with 4 antennas and 6 auxiliary slots. NP and the EVE group tests require a much smaller number of antennas or sensors to reach $P_d \simeq 1$ wrt to all other tests.

VI. Optimization of Hybrid Energy Detection

In this section, we show some preliminary results on the optimization of Hybrid Energy Detection. Let us assume that the secondary user has a fixed time window for both noise estimation and detection, i.e., the number of samples that the SU can use for both noise estimation and signal detection is constant. For the sake of simplicity, the Maximum Likelihood expression of (10) will be considered for the optimization of HED described in IV-B. Considering K antennas, M samples are used for estimation and N samples for detection. Our fixed time constraint implies $M+N = c$ where c is a constant, hence our goal is to find the optimal M (and consequently optimal N) that gives the maximum detection probability.

In [22][23] the mathematical analysis of HED was performed, the false alarm and detection probability expressions are the starting point of our optimization task. The False Alarm Probability $P_{fa}^{(HED)}$ for number of sensors K, number of samples N, number of noise estimation samples M and threshold t is given by,

$$P_{fa}^{(HED)} = Q\left[\frac{t-1}{\sqrt{\frac{M+Nt^2}{KMN}}}\right] \qquad (15)$$

Similarly, the Probability of Detection $P_D^{(HED)}$ in similar scenario is given by,

$$P_d^{(HED)} = Q\left[\frac{(t-1-\rho)}{\sqrt{\frac{t^2}{KM}+\frac{K\rho^2+2\rho+1}{KN}}}\right] \qquad (16)$$

where ρ is the signal-to-noise ratio.

First of all, from (15) we find the threshold t expression

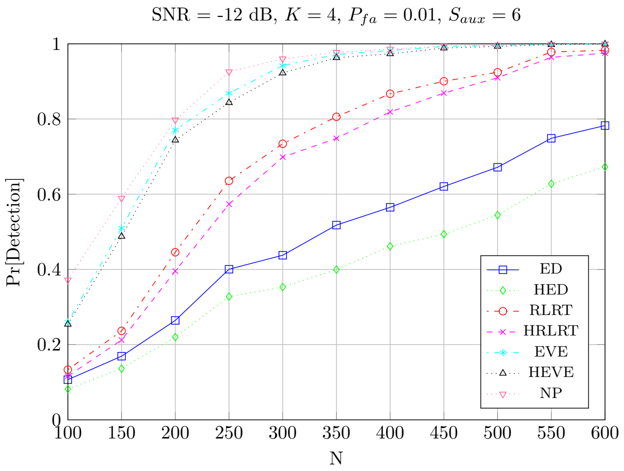

Figure 6. Performance curve, Pd vs. N, $K = 4$

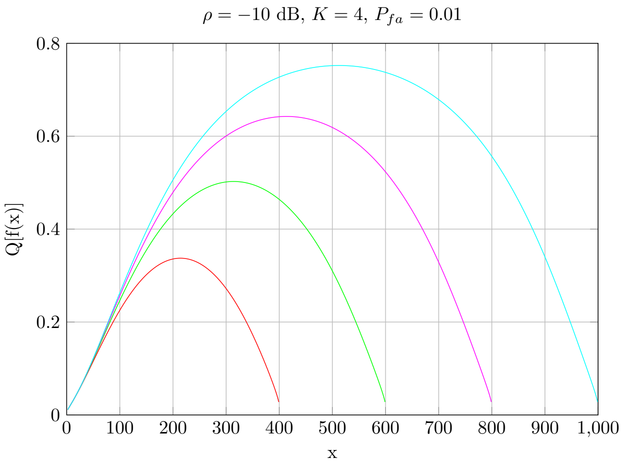

Figure 7. Probability of detection as a function of M given $M + N =$ const.

as a function of the P_{fa},

$$t = \frac{M\left(K + \epsilon\sqrt{\frac{KM+KN-\epsilon^2}{MN}}\right)}{KM - \epsilon^2} \tag{17}$$

where $\epsilon = Q^{-1}[P_{fa}]$. This is the only acceptable solution ($t > 1$) of a second degree equation. Unless KM is smaller than ϵ^2 (which is of no interest), this is always true.

By substituting (17) in (16) we obtain the following expression:

$$P_d = Q\left[\frac{\frac{M\left(K+\epsilon\sqrt{\frac{KM+KN-\epsilon^2}{MN}}\right)}{KM-\epsilon^2} - 1 - \rho}{\sqrt{\frac{M\left(K+\epsilon\sqrt{\frac{KM+KN-\epsilon^2}{MN}}\right)^2}{K(KM-\epsilon^2)^2} + \frac{K\rho^2+2\rho+1}{KN}}}\right] \tag{18}$$

Let us now use the following substitutions:

$$M = x \tag{19}$$
$$N = c - x \tag{20}$$

where $x \in \mathbb{N}$ and $c = M + N$.

We first rewrite the threshold expression in (17):

$$t = \frac{x(K + \epsilon\sqrt{\frac{Kc-\epsilon^2}{xc-x^2}})}{Kx - \epsilon^2} \tag{21}$$

Then, we rewrite the argument of the Q-function of (18):

$$f(x) = \frac{\frac{x\left(K+\epsilon\sqrt{\frac{Kc-\epsilon^2}{cx-x^2}}\right)}{Kx-\epsilon^2} - 1 - \rho}{\sqrt{\frac{x\left[K^2+\frac{\epsilon^2(Kc-\epsilon^2)}{cx-x^2}+2KQ\sqrt{\frac{Kc-\epsilon^2}{cx-x^2}}\right]}{K(K^2x^2+\epsilon^4-2\epsilon^2Kx)} + \frac{K\rho^2+2\rho+1}{Kc-Kx}}} \tag{22}$$

Figure 7 shows the probability of detection of HED as a function of M for different values of $M+N$, with 4 antennas, SNR equal to -10dB and P_{fa} equal to 10^{-2}. It is clear to see that, when c samples are available for both estimation and detection, the highest probability of detection occurs for:

$$M \approx N \approx \frac{M + N}{2} \tag{23}$$

Hence, given a time slot for spectrum sensing, the best performance occurs when estimation and detection slots are equally split.

VII. Conclusions

In this paper, some important classes of multi-antenna spectrum sensing algorithms have been considered. The hybrid approach of method based on the eigenvector of the covariance matrix has been introduced. Performance of the new hybrid test has been compared with the well-known RLRT end ED together with their hybrid approaches HRLRT and HED. It is shown that the EVE test and its hybrid approach are able to outperform RLRT, ED and they respective hybrid approaches, furthermore it can significantly reduce the gap with the NP test. Finally, given a fixed time slot or number of samples for HED, it is concluded that estimation and detection slots should be equally divided in order to achieve the optimal performance.

References

[1] J. Mitola, III, “Cognitive radio. An integrated agent architecture for software defined radio”, Ph.D. dissertation, Royal Institute of Technology (KTH), May 2000.

[2] J. Neyman and E. Pearson, “On the Problem of the Most Efficient Tests of Statistical Hypotheses,” Philosophical Transactions of the Royal Society of London, 1933.

[3] IEEE Standard for Information technology Local and metropolitan area networks Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands, IEEE Std 802.22-2011, July 2011, pp. 1-680.

[4] H. Urkowitz, “Energy detection of unknown deterministic signals,” Proceedings of the IEEE, Apr. 1967, pp. 523-531.

[5] D. Cabric, A. Tkachenko, and R.W. Brodersen, “Spectrum Sensing Measurements of Pilot, Energy, and Collaborative Detection,” Military Communications Conference, IEEE, 23-25 Oct. 2006, pp. 1-7.

[6] Jian Chen, A. Gibson, and J. Zafar, “Cyclostationary spectrum detection in cognitive radios,” IET Seminar on Cognitive Radio and Software Defined Radios: Technologies and Techniques, 18 Sept. 2008, pp. 1-5.

[7] Y. Zeng and Y.-C. Liang, “Eigenvalue-based spectrum sensing algorithms for cognitive radio”, IEEE Trans. Commun., vol. 57, no. 6, 2009, pp. 1784-1793.

[8] W. Zhang, G. Abreu, M. Inamori, and Y. Sanada, “Spectrum sensing algorithms via finite random matrices”, IEEE Trans. Commun., vol. 60, no. 1, Jan. 2012, pp. 164-175.

[9] A. Kortun, T. Ratnarajah, M. Sellathurai, C. Zhong, and C. Papadias, “On the performance of eigenvalue-based cooperative spectrum sensing for cognitive radio”, IEEE J. Selected Topics Signal Process., vol. 5, no. 1, Feb. 2011, pp. 49-55.

[10] S.K. Sharma, S. Chatzinotas, and B. Ottersten, “Eigenvalue based sensing and SNR estimation for cognitive radio in presence of noise correlation”, IEEE Trans. Veh. Technol., vol. 62, no. 8, Oct. 2013, pp. 3671-3684.

[11] L. Cardoso, M. Debbah, P. Bianchi, and J. Najim, “Cooperative spectrum sensing using random matrix theory”, in proc. 3rd Int. Symp. Wireless Pervasive Comp., May 2008, pp. 334-338.

[12] F. Penna, R. Garello, and M. Spirito, “Cooperative spectrum sensing based on the limiting eigenvalue ratio distribution in Wishart matrices”, IEEE Commun. Letters, vol. 13, no. 7, July 2009, pp. 507-509.

[13] S.K. Sharma, S. Chatzinotas, and B. Ottersten, “The effect of noise correlation on fractional sampling based spectrum sensing”, in Proc. IEEE ICC, June 2013, pp. 1182-1187.

[14] Y. Zeng, C. Koh, and Y.-C. Liang, “Maximum eigenvalue detection Theory and application”, in Proc. IEEE ICC, May 2008, pp. 4160-4164.

[15] P. Wang, J. Fang, N. Han, and H. Li, “Multiantenna-assisted spectrum sensing for cognitive radio”, IEEE Trans. Veh. Technol., vol. 59, no. 4, May 2010, pp. 1791-1800.

[16] P. Bianchi, M. Debbah, M. Maida, and J. Najim, “Performance of statistical tests for single-source detection using random matrix theory”, IEEE Trans. Info. Th., vol. 57, no. 4, 2011, pp. 2400-2419.

[17] Y. Zeng and Y. C. Liang, “Maximum-Minimum Eigenvalue Detection for Cognitive Radio”, Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on, 3-7 Sep. 2007, pp. 1-5.

[18] S. Sequeira, R.R. Mahajan, and P. Spasojevic, “On the noise power estimation in the presence of the signal for energy-based sensing,” Sarnoff Symposium (SARNOFF), 2012 35th IEEE, 21-22 May 2012, pp. 1-5.

[19] S.N. Roy, “On a Heuristic Method of Test Construction and its use in Multivariate Analysis,” The Annals of Mathematical Statistics, vol. 24, no. 2, Jan. 1953, pp. 220-238.

[20] P. Bianchi, M. Debbah, M. Maida, and J. Najim, “Performance of Statistical Tests for Source Detection using Random Matrix Theory”, Information Theory, IEEE Transactions on , vol. 57, no. 4, Apr. 2011, pp. 2400-2419.

[21] R. Garello and Y. Jia, “Improving spectrum sensing performance by using eigenvectors”, The First Intl. Conf. on Advances in Cognitive Radio, Budapest, Hungary, Apr. 2011, pp. 26-30.

[22] P. Dhakal, D. Riviello, F. Penna, and R. Garello, “Impact of noise estimation on energy detection and eigenvalue based spectrum sensing algorithms.” IEEE International Conference Communications (ICC), Sydney, Australia, Jun. 2014, pp. 1367-1372.

[23] P. Dhakal, D. Riviello, F. Penna, and R. Garello, “Hybrid Approach Analysis of Energy Detection and Eigenvalue Based Spectrum Sensing Algorithms with Noise Power Estimation,” The Fourth Int. Conf. on Advances in Cognitive Radio, Nice, France, Feb. 2014, pp. 20-25.

[24] B. Nadler, F. Penna, and R. Garello, “Performance of eigenvalue-based signal detectors with known and unknown noise level,” in Proc. of International Conference on Communications (ICC 2011), Jun. 2011, pp. 1-5.

[25] Kritchman, Shira, and Nadler. “Non-parametric detection of the number of signals: hypothesis testing and random matrix theory.” IEEE Transactions on Signal Processing, vol. 57, no. 10, 2009, pp. 3930-3941.

[26] F. Penna, R. Garello, and M.A. Spirito, “Probability of Missed Detection in Eigenvalue Ratio Spectrum Sensing,” IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Commun. (WIMOB), Marrakech, Morocco, Japan, 2009, pp. 12-14.

Jamming Separation in GPS Signals Using Independent Component Analysis

Pedro Luis Araújo Silva
Post-Grad. Prog. in Elec. Engineering, PPgEE – COPELE
Federal University of Campina Grande, UFCG
Federal Institute of Education, Science and Technology of Paraíba, IFPB
Campina Grande – PB, Brazil
e-mail: pedro.silva@ee.ufcg.edu.br

Edmar Candeia Gurjão, Glauco Fontgalland
Department of Electrical Engineering
Federal University of Campina Grande, UFCG
Campina Grande – PB, Brazil
e-mails: ecandeia@dee.ufcg.edu.br ,
fontgalland@dee.ufcg.edu.br

Abstract - **The Global Positioning System (GPS) is a worldwide service use and is used as a reference for many other time base systems, altitude, latitude and longitude. Intentional jammers (jammers) have degraded the reception of GPS signals, causing the receivers to fall out of sync. The technique employed in Independent Components Analysis (ICA) provides the ability to separate and mitigate the interference (jamming). A Software-Defined Radio (SDR) was used to confirm the effectiveness of this technique against jamming.**

Keywords - GPS; jammers; ICA; jamming; SDR.

I. INTRODUCTION

The Global Positioning System (GPS) is one of the most used telecommunications systems, used in various applications like online mapping, car tracking, traffic control, etc. [1]. To avoid the localization of a target by GPS, some portable devices were developed to interfere with localization signal reception.

The received GPS signal normally has a low power, i.e., -160 dBm, with approximately 20 MHz of bandwidth. Thus, a jammer device, that produces the interference signal in the same frequency bands with the GPS signal, can interrupt the signal reception for kilometers [2]. The utilization of these devices are forbidden, but they can be easily acquired in the market [3].

Some techniques have been developed to combat the jammers as adaptive filtering [4][5], filtering in the time - frequency domain [6][7], adaptive antennas [8][9], among others. In this paper, we propose the utilization a blind source separation technique Independent Component Analysis (ICA) to separate the GPS signal from the interference. ICA has an efficient implementation and good performance in the low Signal-to-Noise Ratio (SNR) situations, as is the case of GPS signals.

We used real measurement signal to validate the proposed utilization and the obtained results shows the efficiency of ICA in the GPS signal recovery.

This article is arranged as follows: Section II presents the software-defined radio, in Section III is a brief description of the method of analysis in independent components (ICA). Section IV presents the used software-defined radio. The application of the method proposed in the situation is defined in Section V. Finally, the results and conclusions are in Section VI.

II. SOFTWARE-DEFINED RADIO

The Software-Defined Radio (SDR) is designed as a reconfigurable and flexible arrangement of radio that is based on a software [16]. Thus, it provides the possibility of implementing several radio configurations, only by changing software parameters, taking advantage of the same hardware structure. Moreover, thanks to the high processing power of the platform, one can use a more elaborate signal processing with real-time radio systems in a fast development environment of use applications.

GNU Radio is a free software platform and open source used in the development of hardware without radios in a simulation environment, or with an external RF hardware cost. There are pre-defined blocks in an internal library or created by the user, which operate independently and, when connected, form software-defined radios.

The Universal Software Radio Peripheral (USRP) [17] is an RF device consisting of a motherboard and a set of plates daughters. On-board analog-to-digital converters are in the reception area (path from the antenna to the processing system), digital to analog converters in the transmission zone (path processing system to the antenna) and an FPGA to multiplex data the daughter card from reception to the computer and vice versa.

Each daughter card is designed for a range of frequencies and, in a typical configuration, are arranged into four units: two for transmission and two for reception.

III. INDEPENDENT COMPONENT ANALYSIS

The Independent Component Analysis (ICA) [10] is a blind source separation method, where the base on the linear mixture of signal sources, the objective is to recover a statistically independent and non Gaussian representation of each source.

Consider n statistically independent sources $(s_1, s_2, s_3, \dots, s_n)$ and m measurements of mixture of these sources, $(x_1, x_2, x_3, \dots, x_n)$, written as a linear combination of the sources by

$$x = As. \tag{1}$$

where $$x = (x_1, x_2, x_3, \dots, x_n)^T. \tag{2}$$

is the measurement vector, known a priori. The mixing matrix A and the source vectors,

$$s = (s_1, s_2, s_3, \dots, s_n)^T. \tag{3}$$

are unknown.

If matrix A is known, to recover the source vector s

$$s = A^{-1}x. \tag{4}$$

however as matrix A is not known, it is necessary to estimate a separation matrix W that recover the source vector s, using only the measurement vector x:

$$\hat{s} = Wx = WAs. \tag{5}$$

Figure 1 represents the block diagram of ICA.

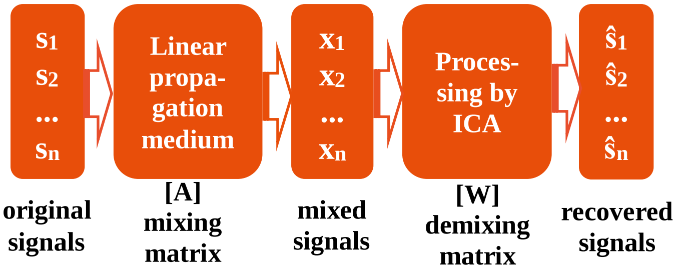

Figure 1. Block diagram of the ICA.

The first step for the application of ICA is to choose a cost function. After, an optimization method to optimize the cost functions must be chosen. In this work, we use an efficient method to perform these tasks, the FastICA [18], which is based on maximizing nengetropia [10], using as cost function the nonlinear function:

$$g = y^3. \tag{6}$$

and symmetrical orthogonalization.

IV. Software-Defined Radio Used

For the verification of the application of ICA result to separate the GPS signal jamming, a software-defined radio was used, GNSS-SDR, proposed in [19]. This radio implements an algorithm for the acquisition and demodulation of the signal and another location algorithm, based on information derived from the first.

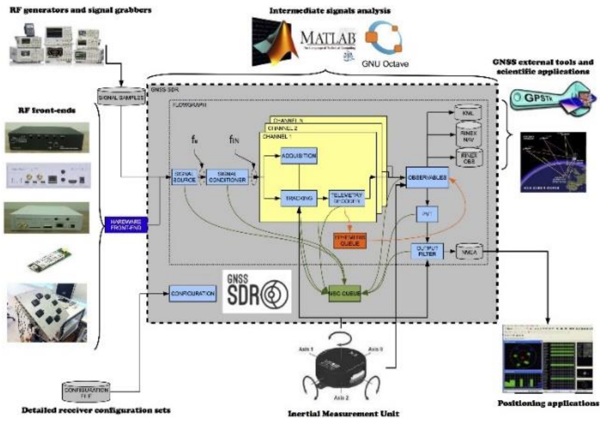

Figure 1 - Overview Software-Defined Radio GNSS-SDR [19].

V. Application of the Method in Proposed Case

To demonstrate the application of the proposed method used a GPS signal from the Crawdad database [11], represented in Figure 3. This signal has central frequency of 1575.42 MHz, sampling rate of 6.4 GHz, span of 5 MHz and 320000 samples were registered. It was acquired using a Tektronix RSA3408A real time spectrum analyzer, a Rojone A-GPSA95NS antenna, Rojone AMA-061B amplifier and a DC blocker.

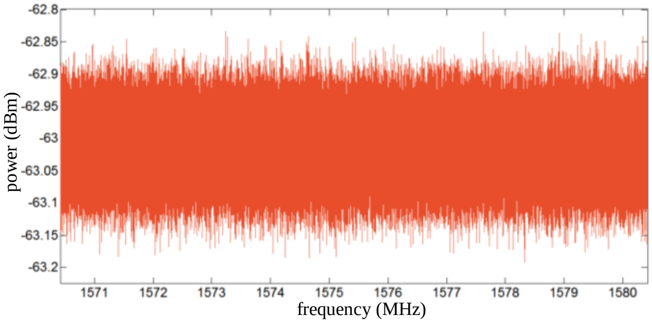

Figure 3. GPS signal spectrum.

As interference signal was used a chirp signal signal, generate using Matlab®, shown in Figure 4. This signal has a central frequency of 1575.42 MHz (GPS L1 Band), initial frequency (f_0) in 1570.42 MHz, final frequency (f_1) in 1580.42 MHz and a quasi static sweeping mode, whose instantaneous frequency is given by

$$f_i(t) = f_0 + (f_1 - f_0)t^2. \tag{7}$$

according to signals emitted by GPS jammers [12][13].

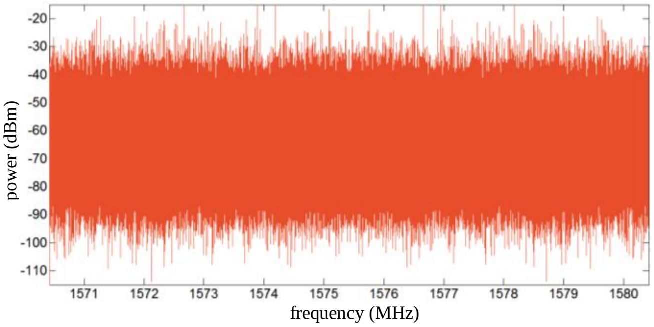

Figure 4. Spectrum chirp signal (interference signal).

FastICA [18] was the algorithm used to separate the mixture of the GPS and Chirp signal. According to [14] and [15], ICA has some restrictions, and one of them is the signal sources have non Gaussian distribution. When the sources are Gaussian there is no guarantee of source recovery. GPS signal has probability distribution near of Gaussian (2.971 kurtosis).

However, when we apply the FastICA to some mixture of GPS signals, the sources were recovered. As ICA does not guarantee prefect recovery of phase, or order of the recovered signal, as shown in [14] and [15], we used the cross correlation to test the signal correspondence between original and recovered signals.

When compared by correlation, the original GPS signal and the first recovered component, shown in Figure 5, the obtained correlation -0.0067.

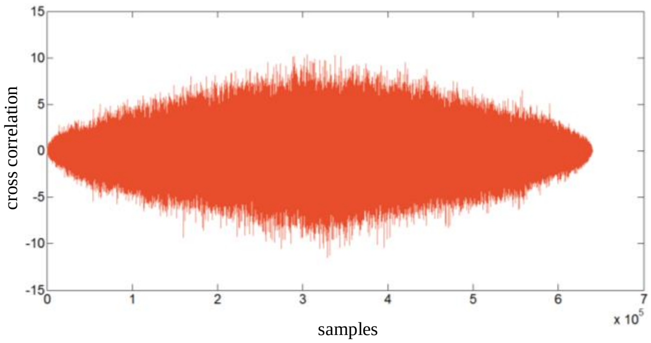

Figure 5. Cross correlation between the original signal and the GPS signal chirp recovered.

Figure 6 shows the cross correlation between the original chirp signal and second recovered component, that gives a correlation coefficient of -0.0049.

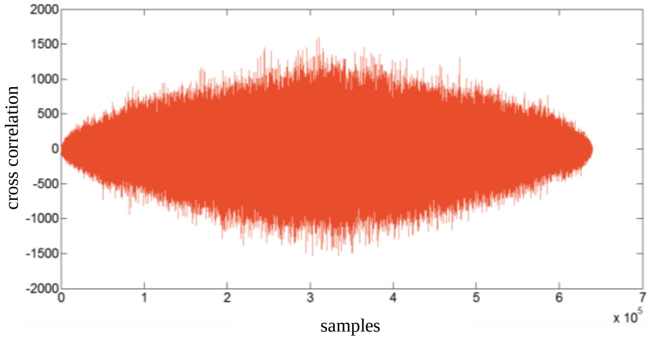

Figure 6. Cross correlation between the original chirp signal and the recovered GPS signal.

The results shown in Figures 5 and 6 indicate the similarity between recovered signals. In the comparison between the original GPS signal and the second recovered component, presented in Figure 7, the correlation coefficient is 0.9987.

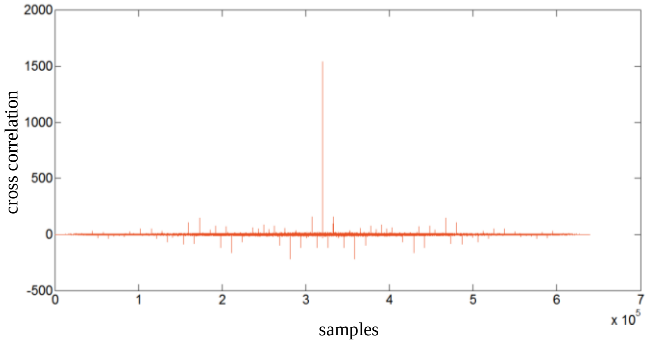

Figure 7. Cross correlation between the original and the recovered GPS signals.

In Figure 8, the comparison of original chirp signal and the first recovered component, the correlation coefficient is -0.9998. In these last comparisons, it was observed that signal has great similarity.

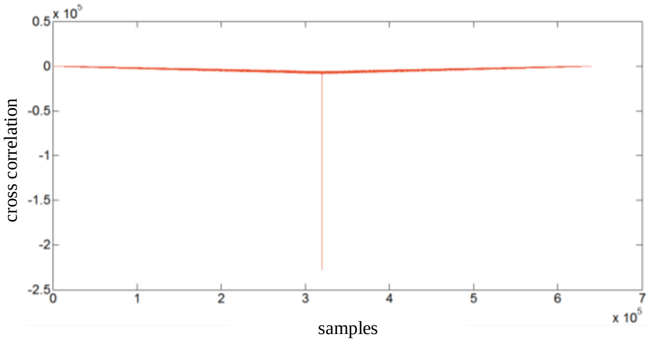

Figure 8. Cross correlation between the original and recovered chirp signals.

As GPS signals has its data modulated by C/A code (a PRN-Code broadcast at 1.023MHz which spreading the data over a 2MHz bandwidth), which in turn modulates the L1 carrier (1575,42 MHz) using Binary-Phase-Shift-Keying (BPSK), the original GPS signal (Figure 9), the mixture of the GPS signal and signal interference (Figure 10) and the recovered GPS signal (Figure 11) were demodulated.

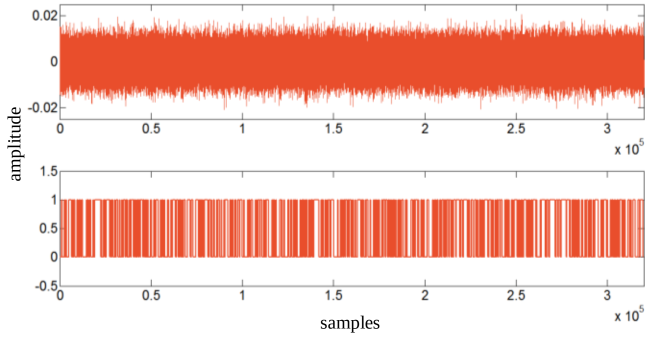

Figure 9. Original GPS signal demodulated.

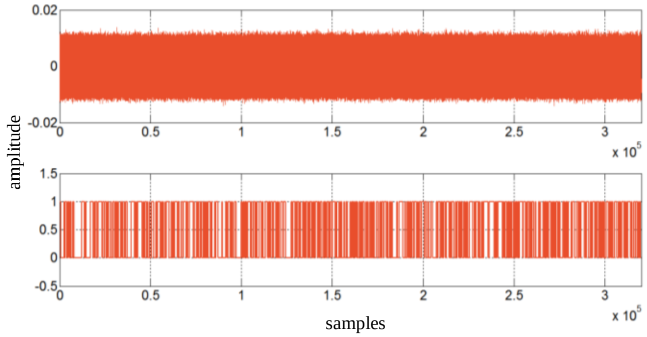

Figure 10. GPS signal mixed to interference and demodulated.

ISBN: 978-1-61208-403-9

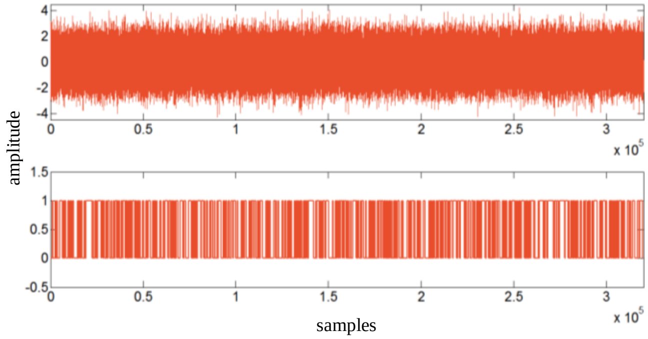

Figure 11. GPS signal demodulated recovered.

After that the correlation coefficient were obtained and the results are original and mixed signal (0.0501), mixed and recovered (0.0434) and original and recovered signals (0.9935).

VI. Results and Conclusion

Since FastICA does not guarantee that the original signals are recovered in the same order, we made four comparisons between the original signals and the signals recovered to detect which pairs of signals corresponded. In this test, it was found that the original GPS signal had a low correlation (-0.0067) with the first independent component and a high correlation (0.9987) to the second one. This indicates that the second independent component of the GPS signal is recovered with the same phase.

Then, it was discovered that the original chirp signal had high correlation with the first independent component (-0.9998) and low correlation with the second (-0.0049). This indicates that the first independent component represents the chirp signal recovered with reversed phase.

To confirm the first conclusion, a second test was done. The test compared three GPS signals between them: the original, the original mixed with interference and the recovered. The correlation between the original and blended signals, and between the mixed with the recovered was low (0.0501 and 0.0434, respectively). This indicates that the compared signals have no similarity. In the confrontation between the original and recovered signals, a high coefficient of correlation was achieved (0.9935), indicating that the signals tested have great similarity.

In this case, it is concluded that the chirp signal actually represented an interference to the GPS signal, as the signal was demodulated when mixed, did not correlate with either the original signal as the recovered signal. Another conclusion, and the most important, is that the analysis in independent component (ICA) was really a tool capable of separating interference (chirp signal) of the desired signal (GPS), since the comparison between the original and GPS signals recovered by ICA, could become a very high similarity.

Finally, as obtained by the RDS-GNSS position coordinates corresponding to the original GPS signals, mixed and recovered, has the following output: the difference between the original coordinates of the extracted GPS signal, and the retrieved signal was only 68 meters, as shown in Figure 12. While the GPS signal mixed with the chirp interference will not return any coordinate point indicating that there was actually a loss of synchronization with the GPS satellites, if the jamming still present.

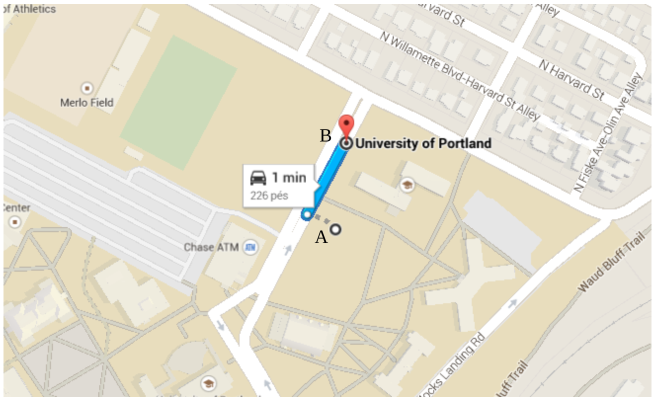

Figure 12. Difference between the original GPS point (A) and recovered point (B).

This work was the result of the first research on the topic in question. In the future, it will continue to be developed, so that consideration be other mitigating interference in GPS signals, such as the multi-jamming and other waveforms.

Acknowledgement

The authors thank the Federal Institute of Education, Science and Technology of Paraíba - IFPB - Campus Campina Grande for the financial support provided to fund the expenses related to the presentation of this work. Thank also to the Federal University of Campina Grande - UFCG and Electromagnetics Laboratory and Applied Microwave - LEMA the possibility of performing this work. In addition, the Higher Education Personnel Training Coordination - CAPES, the scholarship funding during the master program.

References

[1] G. Seeber, “Satellite Geodesy”, 2ª ed., Berlim: Walter de Gruyter, 2003.

[2] E. D. Kaplan and C. J. Hegarty, “Understanding GPS: principles and applications”, 2ª ed., Norwood: Artech House, 2006.

[3] C. Jeffrey, “An Introduction to GNSS: GPS, GLONASS, Galileo and other Global Navigation Satellite Systems”, 1ª ed., Calgary: NovAtel, 2010.

[4] P. S. Diniz, “Adaptive Filtering: Algorithms and Practical Implementation”, 3ª ed., New York: Springer, 2008.

[5] W. L. Mao, C. S. Hwang, C. W. Hung, and J. Sheen, “Narrowband Interference Cancellation using Set-membership Adaptive Predictor for GPS Receiver, Recent Advances in Systems, Control, Signal Processing and Informatics”, 2013, pp. 190-195.

[6] S. Okamura, “The Short Time Fourier Transform and Local Signals”, Dissertations. Pittsburgh, 2011. Paper 58. [Online]. Available from: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1065&context=dissertations. 2015.

02.14

[7] H. You-Guo, G. Wei, and J. Xiao-zhang, “An anti-jamming GPS receiver based on subspace decomposition method”, International Conference on Communication Software and Networks, 2009, pp. 9-12.

[8] Y. Zheng, “Adaptive Antenna Array Processing for GPS Receivers”, Dissertations. Adelaide, 2008. [Online]. Available from: https://digital.library.adelaide.edu.au/dspace/bitstream/2440/49670/1/02whole.pdf. 2015.01.30

[9] R. A. Qamar and N. M. Khan, “Null steering, a comparative analysis”, Multitopic Conference, 2009. INMIC 2009. IEEE 13th International, 2009, pp. 1-5.

[10] A. Hyvtirinen, J. Karhunen, and E. Oja, “Independent Componen Analysis”, New York: Wiley, 2001.

[11] J. P. Hoffbeck and A. Melton, “Data set of RF recordings of several communication signals captured by a real time spectrum analyzer”, Crawdad. [Online]. Available from: http://crawdad.cs.dartmouth.edu/up/rf_recordings/. 2015. 02.18

[12] T. Kraus, R. Bauernfeind, and B. Eissfeller, “Survey of in-car jammers - analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation) ”, Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION/GNSS), 2011, pp. 430-435.

[13] R. H. Mitch et al, “Signal characteristics of civil GPS jammers”, Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION/GNSS), 2011, pp. 1907-1919.

[14] P. Comon and C. J. Eds, “Handbook of Blind Source Separation, Independent Component Analysis and Applications”, Oxford: Academic Press, 2010.

[15] J. V. Stone, “Independent Component Analysis: A Tutorial Introduction”, Cambridge: MIT Press, 2004.

[16] E. Grayver, “Implementing Software-Defined Radio”, Springer, 2013.

[17] Ettus Research, “Universal Software Radio Peripheral: The Foundation for Complete Software Radio Systems”,[Online]. Available from: http://www.upc.edu/sct/documents_equipament/d_174_id-459.pdf. 2015.03.01

[18] A. Hyvarinen and E. Oja, “Independent Component Analysis: Algorithms and Applications”, Neural Networks Research Centre - Helsinki University of Technology. New York: Wiley, 2001.

[19] C. F. Prades, J. Arribas, L. Esteve, D. Pubill, and P. Closas, “An open source Galileo E1 software receiver”, Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2012, pp. 1-8.

■