RIELAC, Vol. XXXVIII 2/2017 p. 36-48 Mayo – Agosto ISSN: 1815-5928

RIELAC
Revista de Ingeniería Electrónica, Automática y Comunicaciones

Modeling cooperative communications using game theory: applications for cognitive radios

Luis M. Gato Díaz, Meiby Ortiz Bouza and Jorge Torres Gómez

ABSTRACT

In this paper, cooperative communications are presented to improve efficiency toward the use of telecommunication systems resources. In the special case of cognitive radio networks, main benefits and costs regarding cooperation are analyzed, as well as security issues that might rise in such a scenario. From a game theory model, the implementation of a coalitional game is described, where cognitive users pursue individual benefits as well as benefits for the coalition they belong. Simulation results confirm the gains achievable by means of cooperative communications, and reveal weakening performance in presence of security threats. This paper may help readers to have a more comprehensive understanding of cooperative communications based on game theory, as well as the main research trends and challenges in this area.

Key words: Cognitive Radio, Cooperative communications, Game theory.

1.- INTRODUCTION

In our daily lives, smart mobile phones are essential electronic devices with virtually unlimited potential for telecommunications. Communicate several points around the world has never been so simple, cheap and high-quality. Nevertheless, the exciting appearance of high-definition applications such as high-definition video streaming continue to challenge an increasing demand for higher data rate wireless access. In this regard, it is expected for 2020 a global mobile data traffic of about 200 times the traffic experienced in 2010 [1]. According to a recent study, carried out by Cisco Systems ®, about 75 % of data traffic volume will be due to video traffic [2]. Another exciting field in the near future is expected to be the Internet-of-things (IoT), where wireless sensor networks [3] and machine-to-machine (M2M) communications [4] are some examples of technologies with overwhelming demand of resources.

With the dramatic grow of mobile data traffic, the efficiency on the utilization of available resources has been set into the spotlight. For instance, frequency spectrum represents a natural resource that has been systematically underutilized due to inefficient spectrum allocation policies. In this regard, dynamic spectrum access along with adaptive bandwidth provision may alleviate the scarcity of frequency spectrum. Further development of mobile technology will be addressed on resource allocation based on awareness of content, user, and location. This technology is expected to solve frequency licensing and spectrum management problems [2]. These attractive features imply a novel concept for wireless communications technologies given by cognitive radio networks [5]. At the same time, cognitive radios are sustained over a software defined radio (SDR) platform in order to perform observation, reconfiguration and cognition [6].

In this paper, the feasibility of wireless cooperative communications in the context of cognitive radio networks is analyzed, to improve efficiency in the use of resources provided by modern communication systems. The objective of cooperation is to optimize the available resources to benefit user communication capabilities. Due to the common interest of each individual user in this scenario, it is appropriate to model their behavior by means of Game Theory [7]. Additional approaches have been reported recently, for example those inspired on biological conducts of some animals [8] and insects [9, 10]. The resources to be optimized can be diverse: spectral frequencies for unlicensed users [11], energy for wireless sensor networks [3], antennas for a virtual multiple-input-multiple-output (MIMO) system [12], etc.

The rest of the paper is organized as follows. In section 2, game theory models for coalitions formation are presented as a convenient way of cooperation among mobile users. In section 3, the main benefits of cooperation are summarized, as well as main drawbacks related that might be significant to some applications. As well as in conventional wireless communications, this novel perspective can be vulnerable to attacks and other security issues, some of which are specific of the cooperation paradigm. In section 4, some of these issues are addressed and classified according to the phase of the cognitive cycle. To provide a practical perspective of all of these matters, a set of simulations of a cooperative communication system exposed to attacks has been conducted. Such scenario is described in section 5, and numerical results obtained are presented as well. A discussion about the scope and limitations of the approach described here is conducted in section 6, where future work directions are revealed. The main conclusions of this investigation are summarized in section 7.

2.- COALITIONAL GAMES FOR COOPERATION

Game theory is a branch of applied mathematics frequently used in economics and in social sciences. Nevertheless, it has been applied to several other disciplines such as political science, biology, computer science, philosophy, and lately, in wireless communication networks [7]. In the latter field, it has been used to solve problems that require decision-making rules, for example: video streaming over mobile networks, ubiquitous Internet access, simultaneous use of multiple technologies, peer-to-peer file sharing, etc.

Cooperative game theory provides analytical tools to study the behavior of rational players when they cooperate. In a cooperative scenario, players are allowed to form agreements among themselves that may impact their strategic choices as well as their utilities [7]. In this section, the object of study is a specific type of game that reinforces cooperation as a way to improve individual and collective benefits that cognitive users get: a *coalitions-formation game* or *coalitional game*. A scenario of a coalitional game for unlicensed users is illustrated in Fig. 1.

Let *K* be the number of cognitive devices in the network, such that the grand coalition is the coalition formed by all of them, and let v be the utility function that rules the game. In a coalitional game *(K, v)*, it is allowed to form a partition S of M mutually disjoint coalitions of *K* [12]. A preference operator (|>) is defined in order to compare the benefits of any pair of possible partitions $S = \{S_1, S_2, \dots, S_M\}$ and $W = \{W_1, W_2, \dots, W_L\}$, comprised by M and L coalitions, respectively. Thus, $S \mid> W$ implies that partition S is preferred over partition W, according to the utility function v. Individual value orders perform the comparison using the individual payoffs such as the Pareto order [12]. Let $\phi_j^v(S)$ and $\phi_j^v(W)$ be the payoffs of player j in partitions S and W, respectively, and let *(K, v)* be a non-transferable utility game, i.e., individual payoffs correspond to the utility of the coalition they belong. The Pareto order is defined as:

$$S \mid> W \overset{\text{if and only if}}{\Longleftrightarrow} \{\phi_j^v(S) \geq \phi_j^v(W) \ \forall j \in S, W\}, \tag{1}$$

which demands individual benefits if at least one strict inequality (>) applies to one player [12]. Based on these principles, an algorithm for conveniently merge and split coalitions must be specified. This enables dynamic regrouping of cognitive devices in new coalitions depending on variable conditions, for example: changes on the utility of the coalition due to mobility of devices, new devices joining the game or some devices leaving the game, etc.

Other subjects to deal in the design of a game-theory-based cooperative system are: the rules to divide the utility $v(S_i)$ among M members of coalition S_i [12], the stability of a partition [7], to define the utility function as well as a cost function [3], and to decide how decisions are made (distributed or centralized) [7].

Depending on the application and its constraints, several utility and cost functions can be defined. For instance, consider the scenario of unlicensed users. The utility must be favorable by the increase of the probability of primary user detection, in order to mitigate interference. On the other hand, cooperation can be prejudicial if the cost incurred is excessive. That is the case when sensing time is so significant that data rate gets deteriorated. In this case, a trade-off is established regarding utility and cooperation issues. For instance, in wireless sensor networks, cooperation may not be affordable if energy consumption is excessive, since most of these devices are power-limited (e.g., due to a short battery life). For the specific case of cognitive radio networks, a commonly used utility function depends on the detection and false-alarm probabilities by the following relation [7]:

$$v(S_i) = Q_{S_i}^{det} - \mathcal{C}\left(Q_{S_i}^{fal}\right) \tag{2}$$

where $Q_{S_i}^{\text{det}}$ and $Q_{S_i}^{\text{fal}}$ are the probabilities of detection and false alarm achieved by coalition S_i, and $\mathcal{C}$ is a cost function of the false alarm probability. This cost function is usually defined as a logarithmic function of the form:

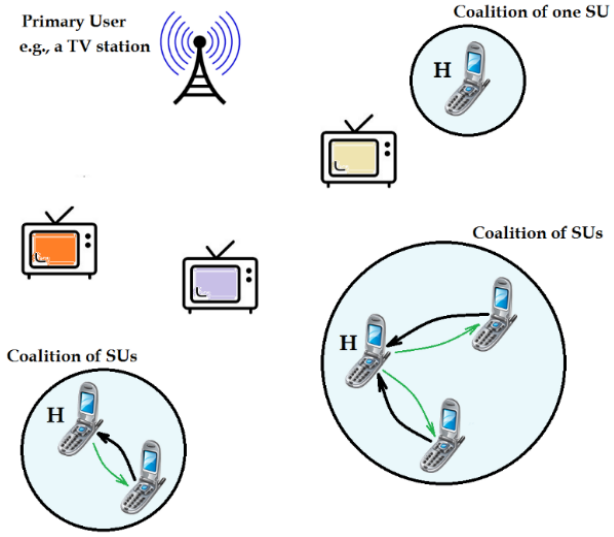

Figure 1

Sample scenario of a coalitional game for unlicensed users (i.e., secondary users: SUs). The coalition head has been specified with an "H". The black and the green arrows indicate the *uplink* and *downlink* control channel, respectively.

$$\mathcal{C}\left(Q_{S_t}^{\text{fal}}\right) = \begin{cases} -\alpha^2 \log\left(1 - \left(\frac{Q_{S_t}^{\text{fal}}}{\alpha}\right)^2\right) & , \quad \text{for } Q_{S_t}^{fal} < \alpha \\ \infty & , \quad otherwise. \end{cases} \tag{3}$$

The cost function is characterized by a barrier-penalty for the probability of false alarm of coalitions, denoted by α. For the coalitional game considered, the expressions[1] for $Q_{S_i}^{\text{det}}$ and $Q_{S_i}^{\text{fal}}$ are as follows [7]:

$$Q_{S_i}^{\text{det}} = 1 - \prod_{j \in S_i} \left((1 - P_j^{det})(1 - P_j^{\text{err}}) + P_j^{det} P_j^{\text{err}} \right) \tag{4}$$

$$Q_{S_i}^{\text{fal}} = 1 - \prod_{j \in S_i} \left((1 - P_j^{\text{fal}})(1 - P_j^{\text{err}}) + P_j^{\text{fal}} P_j^{\text{err}} \right) \tag{5}$$

It has been employed in (4) and (5) the notation P_j^{fal} and P_j^{det} for local probability of false alarm and local probability of detection for the j-th user, respectively. The error probability of transmission of sensing results from the j-th user to the fusion center is [7]:

$$P_j^{\text{err}} = \frac{1}{2} - \frac{1}{2} \sqrt{\frac{\gamma_j^*}{1+\gamma_j^*}} \tag{6}$$

where γ_j^* is the average signal-to-noise ratio (SNR) over the reporting[2] channel, as perceived by the j-th user. The fusion center is selected to be the user with higher local probability of detection [7] and has been marked with an "H" for the coalitions in Fig. 1.

A challenging issue regarding coalitional games is given by the overwhelming amount of computations required to dynamically update the utilities for every possible partition. The number of ways a set of N elements can be partitioned into nonempty subsets is called a Bell number and is denoted B_n. The Bell numbers can be generated using the following recurrence relation [14]:

$$B_{n+1} = \sum_{k=0}^{n} B_k \binom{n}{k}, \text{ with } B_0 = 1 \tag{7}$$

where $\binom{n}{k} \equiv \frac{n!}{(n-k)!\,k!}$ is a binomial coefficient. The first few Bell numbers for $n = 1, 2, 3, 4, 5 \ldots$ are $1, 2, 5, 15, 52, \ldots$ For instance, a set of 10 players would require to evaluate 115975 times the utility function, in order to decide which partition

[1] Actually, expressions (4) and (5) are valid only if the fusion rule used by the coalition head is an "OR" hard-fusion rule. For other fusion rules (e.g., AND-rule, majority-rule, etc.), other expressions are employed. See [13] for further details.

[2] In this paper, words such as "reporting" and "control" are indistinctly used when referring to the reporting channel in a cognitive radio network.

is optimal at a specific time instant. Nevertheless, typically there are some partitions that are usually inopportune (e.g., the grand coalition), and thus can be obviated. In some cases, the overhead may be still affordable when decisions are centralized and the amount of users in the network is not that huge. By way of example, consider the scenario where there exists a secondary base station, and this base station must decide which partition is the optimal and then report to mobile users. This may not be reasonable for an open scenario, due to the associated overhead. An alternative approach is to evaluate the utility of one possible partition (or any possible sub-set of coalitions) at a time, and apply it if the utilities get improved, even when this changes are not necessarily the optimal solution. This method becomes a sequence of merge and split procedures, pursuing better payoffs for the players. See, for instance, [12, 15]. A convenient solution to this problem is to evaluate the utility function in a distributed manner, sharing the overhead among all users in the network. Players may calculate their own utility function for all possible deviations, as was recently proposed in [16].

3.- COOPERATIVE COMMUNICATIONS: BENEFITS AND COSTS

Cooperative communications have been extensively studied in the last few years. Two typical samples of cooperative communication approaches are Amplify-and-Forward and Decode-and-Forward [17]. However, in a cognitive radio network, cooperation can be more sophisticated and may produce further benefits in terms of transmission rate or throughput, reliability, energy efficiency, spectral efficiency, hardware requirements, reduced interference, among others. A comprehensive description of them can be found in [7, 13, 17, 18].

Improvement in data rate or throughput is achieved by reducing the spectrum sensing time. The interference to primary users is mitigated by a more accurate detection. Higher energy efficiency and thus a longer battery life is attained by reducing power consumption due to spectrum sensing periods. Moreover, cooperation enables a dynamic network structure in order to react to environmental conditions. Besides, through cooperation, secondary users may overcome multipath fading, shadowing and receiver uncertainty by taking advantage of spatial diversity. All of these issues are summarized in the cooperation gain quantity. For instance, consider a cognitive radio network which nodes operate as secondary users and send data in the uplink of a Time Division Multiple Access (TDMA) system, as shown in Fig. 2. In such scenario, each transmitter sends data in a specified slot.

The sensing/sharing time includes: local spectrum sensing, an uplink for the local decision and a downlink for the global decision (both over the control channel). Given the slot duration, denoted by T, and the sensing/sharing time, denoted by T_s ($T_s < T$), then the average throughput for a secondary user when the spectrum is idle and when the spectrum is occupied are:

$$\tau_j^{\mathcal{H}_0} = \frac{T-T_s}{T}\left(1 - P_j^{fal}\right)R_j, \tag{8}$$

and

$$\tau_j^{\mathcal{H}_1} = \frac{T-T_s}{T}\left(1 - P_j^{det}\right)R_j, \tag{9}$$

respectively. In (8) and (9), P_j^{fal} and P_j^{det} are the local false-alarm and detection probabilities for the j-th user, respectively, while R_j is its data rate [7]. The supra-indexes $\mathcal{H}_0$ and $\mathcal{H}_1$ are the usual notations for the hypothesis of vacant channel and busy channel, respectively. In this model, the not-sensing/sharing time ($T - T_s$) is assumed to be entirely devoted to transmission, i.e., the switching time is negligible. Moreover, there must be no additional modes of operation others than the transmission and sensing/sharing modes.

A higher data rate is beneficial, but secondary user's transmissions when the primary user is still active is disapproved, since it causes interference. In other words, it is desirable to increase $\tau_{\mathcal{H}_0}$ and reduce $\tau_{\mathcal{H}_1}$. For this purpose, false alarm probabilities must remain low while the detection probabilities are increased, as can be concluded from (8) and (9). This goal is achieved whenever multiple secondary users cooperate and share sensing results in order to improve sensing accuracy. For instance, thanks to the spatial diversity reached through cooperation, cognitive radio networks can mitigate the effects of shadowing or the hidden-terminal problem. The entire network successfully becomes aware about its operating environment by collecting information of the network as a whole, and not from individual nodes only.

Similarly, cooperative spectrum sensing in cognitive radio networks relaxes sensitivity requirements for single terminals, since the capability of detecting weak signals is improved by means of cooperation. Without cooperation, a higher accuracy

during detection of primary users is attained if every cognitive radio individually increases its sensing time T_s in order to improve the signal-to-noise ratio (SNR) [18]. This might[3] reduce the interference rate $\tau_{\mathcal{H}_1}$, although the transmission time is compromised.

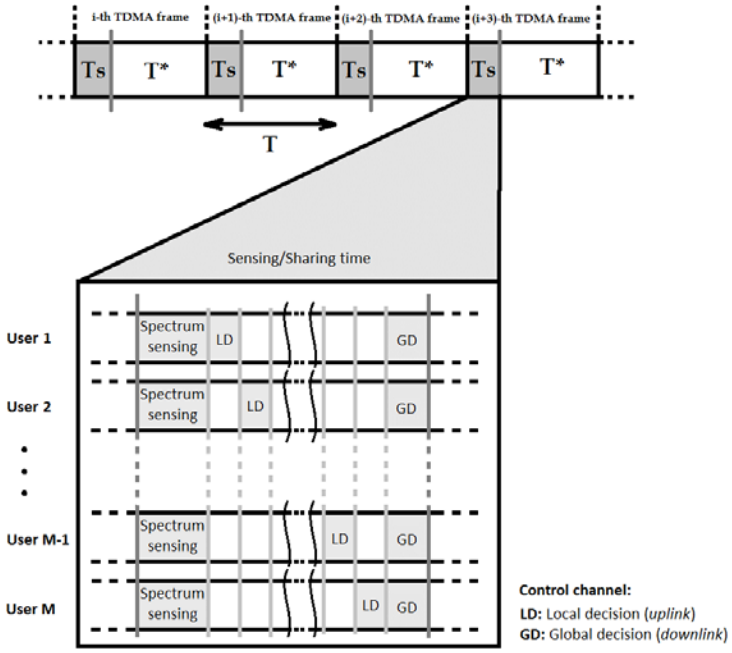

Figure 2

Sample sequence of TDMA frames for a cognitive radio network. For each slot of duration T, there is a sensing/sharing period T_s, and a data transmission period $T^* = T - T_s$. The sensing/sharing time includes: local spectrum sensing, an uplink for the local decision and a downlink for the global decision.

Cooperation can also lead to a reduced sensing time T_s, and thus an increased average throughput, while maintaining the detection and false alarm probabilities at the target levels. In a cooperative communication scheme, efficiency of cooperative sensing is settled by sensing scheduling. Sensing scheduling determines how often secondary users cooperate with each other. Additionally, sensing time can be adjusted from one turn to the next, depending on the accuracy requested, which can be fast sensing or fine sensing [13].

Despite the benefits referred above, cooperative communications may incur in an excessive overhead that limits the achievable gain from cooperation. This overhead can be extra energy consumption and substantial delay due to the reporting channel that supports the cooperation scheme. In some cases, the vulnerability to security attacks may also be part of the cooperation overhead [13]. Although the cooperation overhead becomes decisive, in some particular applications it is considered a challenging matter. In wireless sensor networks, where the efficiency in the use of the battery life is a key factor, extra delays due to cooperation overhead may not be serious, but extra energy consumption may not justify cooperative gains. On the other hand, for high demanding multimedia applications, a negligible delay is critical for the quality-of-service (QoS) even when there were no fundamental restrictions regarding the energy wasted.

These subjects have been the focus of research in recent years and promising results have been achieved. For example, the authors in [31] propose a model in which several secondary users measure a particular channel with non-identical sensing times and a spectrum sensing schedule is designed. Energy consumption is carefully adjusted. The work in [32] proposes a model in which particular sensing duration for each user/channel pair is designated for a higher energy efficiency. Two fundamentals objectives are focused: to minimize the energy consumption and to minimize the spectrum sensing period, saving more time for data transmission. In [33], the authors have established a model of evolutionary game between

[3] In practical scenarios, increasing the sensing time does not necessarily imply a higher detection performance. With a higher sensing time it becomes more likely that primary signals don't last for an entire observation period, and thus a better detection performance is not guaranteed. Additionally, because of the existence of an SNR wall, the detection performance cannot be perpetually improved by increasing the observation period [35].

cognitive sensors. In order to let cognitive sensors to measure a channel effectively, they designed a contribution-punishment mechanism and introduced periodic sleep-listen mechanism. The former stimulate high SNR sensors to participate in spectrum sensing more than low SNR sensors. Each user turns off its radio for some time and wake up and listening if the channel has been occupied. In [34], a utility function which considers the spectrum-efficiency and the energy-efficiency is used. A novel frame structure for cooperative spectrum sensing is introduced, in which the reporting time of one secondary user may overlap the sensing period of the others. They extend the sensing duration utilizing the reporting time without introducing additional time overhead.

Several examples of practical scenarios for wireless communication networks, where cooperation is crucial for resources optimization, has been summarized in [7]:

- **Downlink beamforming in an interference channel:** Enabling wireless systems to efficiently operate in the same spectral band.
- **Multimedia resource management:** Ensuring the required QoS parameters for resource-demanding applications such as multimedia streaming, video surveillance, and video gaming over bandwidth-constrained network infrastructures.
- **Rate allocation in a multiple-access channel:** Fairly allocating, between a number of users, the total transmission rate available in a wireless multiple-access channel.
- **Formation of virtual multiple-input-multiple-output (MIMO) systems:** Single-antenna users cooperating and sharing their antennas in order to benefit from spatial diversity or multiplexing.
- **Exchange of information on intelligent transportation systems:** Vehicle-to-vehicle (V2V) and vehicle-to-road (V2R) cooperation in order to optimize the traffic.

4.- SECURITY ISSUES IN A COOPERATIVE SCENARIO

Cognitive radio architecture is comprised by a set of hierarchical and temporally organized rules that constitute the cognition cycle [5]. Firstly, each cognitive user senses and perceives the environment ("Observation phase"). Then the significance of the observation is evaluated ("Orient phase"), based on some previous observations, for instance. Depending on the priority established, three possible phases are conducted. For a normal priority, an incoming network message is handled by generating a plan ("Plan phase"). For an urgent priority, the cognitive user makes a decision among the candidate plans ("Decision phase"). For an immediate priority, externally or internally oriented actions are conducted ("Acting phase"). Finally, the whole cycle is performed in a learning mechanism [5].

Among the different phases of the cognitive cycle, the observation phase and the acting phase are the most important from a security point of view, since they are the most vulnerable to attacks [19]. During the observation phase, malicious users[4] can intentionally introduce spoofing signals into vacant channel in order to reduce the transmission opportunities of secondary users. In the acting phase (secondary users' transmissions), the adversaries can intentionally do jamming over the communication channel or the reporting channel, and therefore decrease the channel capacity.

The rest of the cognitive cycle depends on internal procedures and, in general, it can only be compromised if an adversary is able to install malicious software on the SDR-based devices. SDR terminals must be able to download new radio applications or waveforms and, once activated, the radio application will change the radio transmission parameters and the internal states of the device. In this regard, two main security issues must be considered [6]: to guarantee that the downloaded software comes from a trusted source, and to guarantee that the downloaded software will behave as expected. However, security issues of this kind are out of the scope of this paper, thus only the observation and acting phases of the cognitive cycle are considered.

Most of the traditional security threats presented in modern wireless communications still apply to wireless cooperative communications. For instance, [19, 20]:

- *receiver jamming*: an attacker reduces the SNR by transmitting noise over the sensing channel;
- *eavesdropping*: unauthorized users get access to exchanged private data;
- *MAC-layer attacks*: malicious users intentionally oversaturate the control channel with irrelevant data;
- *APP-layer attacks*: attacks by means of malwares and viruses;
- *authorization and authentication (A&A) attacks*: vulnerability due to lack of authentication in the cooperation protocol.

[4] In this paper, as well as in references consulted, terms such as "malicious user", "adversary" and "attacker" are indistinctly used. In some cases, when the attacks involve malicious software, a more common term in the security jargon is "cracker".

However, there are some cognitive-radio-networks-specific security vulnerabilities that must be addressed in a cooperative scenario. This second group includes [20]:

- *control channel jamming*: similar to conventional jamming, but over the control/reporting channel;
- *incumbent emulation (IE) attacks*: adversaries imitating the primary user's communication pattern and waveform;
- *spectrum sensing data falsification (SSDF)*: attackers act as legitimate nodes but intentionally report false spectrum sensing data;
- *intruding malicious nodes and selfish nodes*: authenticated and authorized members of the network intentionally report wrong sensing data for their own benefit.

This latter behavior must be carefully considered in the game theory model for cooperation. In the utility function employed in the game, an incentive must be established for solidarity among cognitive users. At the same time, a penalty can be settle down for those users that refuse to cooperate. In evolutionary games (where cooperation is not mandatory), this reward-penalty mechanism has already been formalized, see for example [21-23].

4.1.- SECURITY THREATS IN THE OBSERVATION PHASE

During the observation phase in a cooperative network, malicious users can intentionally conduct spectrum sensing data falsification (SSDF). In this regard, Byzantine attacks have been widely studied as a way of reducing the throughput of the network. The two main objectives of these attacks are [24]:

- *Exploitation*: Increasing the probability of false alarm by reporting that the channel is busy when the sensing results indicate that the channel is actually vacant. This behavior deteriorates the data rate $\tau_{\mathcal{H}_0}$, as can be seen from (1).
- *Vandalism*: Reducing the probability of detection by reporting channel vacancy when the sensing results indicate that the channel is actually busy. This behavior increases the interference rate $\tau_{\mathcal{H}_1}$, as can be seen from (2).

Both attacks, exploitation and vandalism, attempt to obstruct the availability of network's resources for devices or individuals when needed. A detailed description of Byzantine attacks and several countermeasures can be found in [24, 25].

Another malicious pattern that can be found in cooperative communications is the presence of greedy or selfish nodes. In a similar way to the exploitation behavior in a Byzantine attack, selfish users continuously report that a specific spectrum hole is occupied by a primary user. The goal of these users is to monopolize this specific band by forcing other users to evacuate it [25].

4.2.- SECURITY THREATS IN THE ACTING PHASE

As mentioned above, the acting phase is that period of time in which cognitive users perform transmissions over the licensed channel. Besides, transmissions over the reporting channel may be considered part of the acting phase, since in both cases the devices do broadcast. In this phase, the main vulnerability found is the chance for the adversaries to intentionally produce interference, and thus to deteriorate the communications channel or to obstruct the cooperation protocol. In this paper, those attacks are referred as "jamming" in general. A comprehensive study of jamming attacks and *jamming* mitigation in cognitive radio networks can be found in [26].

Anti-jamming defense mechanisms based on game theory have been proposed, as an advance method to enforce security in the network, see for example [27-29]. This games are usually modeled as zero-sum, since both the cognitive users and the attacker are supposed to have opposite objectives.

5.- PERFORMANCE EVALUATION OF A COOPERATIVE SYSTEM UNDER ADVERSE CONDITIONS

Let's consider a set of four secondary users allowed to share a common spectrum frequency band with a licensed user. In order to coexist with the primary user of this channel, secondary users must frequently sense the spectrum to avoid interference. There are several detection methods for spectrum sensing, and most of them have been described in [13]. For simulation purposes, let's consider energy detection. It is the most used method for spectrum sensing, thanks to its affordable complexity and its capability to perform non-coherent detection [30].

The spectrum sensing problem can be stated in terms of a binary hypothesis test, where $\mathcal{H}_0$ represents the hypothesis corresponding to the absence of the signal of interest (SoI), and $\mathcal{H}_1$ to the presence of the SoI. For a communication

channel characterized by additive white Gaussian noise (AWGN), and a detection based on N samples of the received signal, these hypotheses are:

$$\begin{aligned} \mathcal{H}_0: \quad x[n] &= \omega[n] \\ \mathcal{H}_1: \quad x[n] &= s[n] + \omega[n] \end{aligned} \qquad \text{for } n = 0, 1, \dots, N-1 \tag{10}$$

where $x[n]$ and $s[n]$ represent the received signal and the SoI, respectively. The channel noise is denoted by $\omega[n]$, which variance σ_ω^2 is supposed to be known. Other channel effects such as fading and shadowing can be considered in this model, however, they are out of the scope of this paper. One possible decision statistic for energy detection is [30]:

$$E = \frac{1}{N}\sum_{n=0}^{N-1}\left(\frac{x[n]}{\sigma_\omega}\right)^2 \tag{11}$$

This value is compared to a local threshold η_j that depends on the local false-alarm probability of the j-th user, $P_j^{fal} = P\{E > \eta_j | \mathcal{H}_0\}$. According to the Neyman-Pearson criterion, the following relation is applied [30]:

$$\eta_j = \sqrt{2N}\, Q^{-1}\left(P_j^{fal}\right) + N \tag{12}$$

The local false-alarm probability is a design parameter, matching application-specific requirements. On the other hand, the local detection probability $P_j^{det} = P\{E > \eta_j | \mathcal{H}_1\}$, can be expressed as [30]:

$$P_j^{det} = Q\left(\frac{\eta_j - N(1+\gamma_j)}{\sqrt{2N(1+\gamma_j)}}\right) \tag{13}$$

where γ_j is the average SNR over the sensing channel, as perceived by the j-th secondary user. In (12) and (13), functions Q and Q^{-1} are the complementary Gaussian distribution function and its inverse function, respectively.

The amount of partitions that can be formed from a set of four users is the fourth Bell number, $B_4 = 15$, as can be obtained from (7). The parameters employed during simulations are summarized in Chart 1. In simulations, a particular case is considered: each SU perceives a 30 dB higher SNR in the reporting channel than in the sensing channel. To address the game-theoretic dynamic, a cognitive base station (CBS) is included, which operates over the reporting channel. For the sake of simplicity of the cooperation protocol, a centralized fusion scheme is employed. The reader may check that this consideration is not restrictive and that all the following results remain true if a non-centralized scheme is used.

Chart 1
Simulation parameters for the coalitional game under study

Parameter:	Value:	Description:
M_{PU}	1	Number of primary users.
M_{SU}	4	Number of secondary users.
P_j^{fal}	0.001	Local false-alarm rate. It is the same for every secondary user.
α	0.010	Penalty-barrier. It is a parameter of equation (3).
N	512	Number of samples used by the energy detector.
γ_j	SU_1: 0 dB; SU_2: -6 dB; SU_3: -8 dB; SU_4: -10 dB	Signal-to-noise ratio over the sensing channel.
γ_j^*	$\gamma_j + 30$ dB	Signal-to-noise ratio over the reporting channel.

Simulation starts from partition $S = \{S_1, S_2, S_3, S_4\}$ as shown in Fig. 3 (a), that represents a non-cooperative scenario. After computing their individual payoffs for every possible partition, the CBS decides that the three worst positioned users must cooperate by forming a coalition, as shown in Fig. 3 (b). The coalition formation algorithm applied by the CBS is depicted in Chart 2.

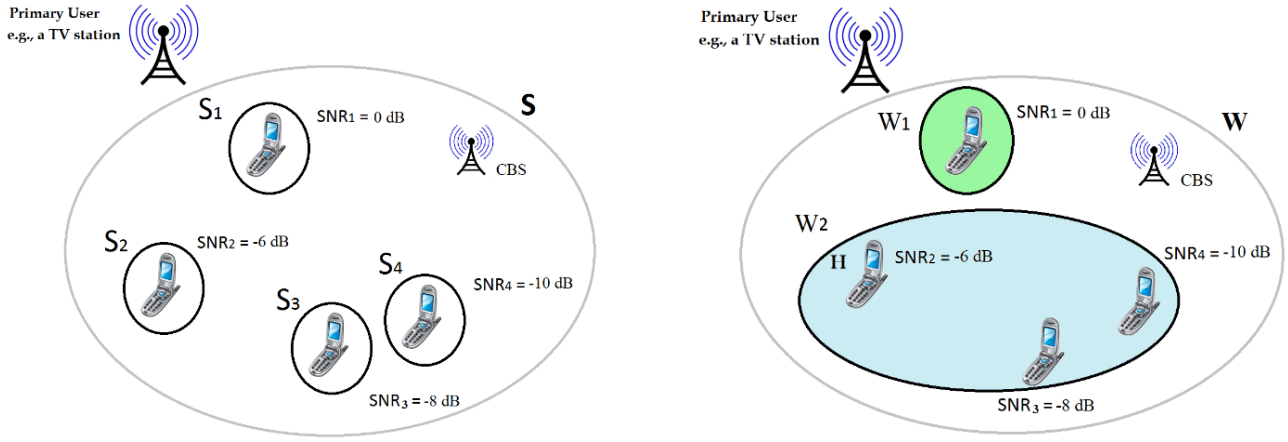

Figure 3

Coalitions formation for the simulation parameters in Chart 1: (a) Non-cooperative scenario, and (b) Secondary users with the lowest P^{det} decide to cooperate in order to improve their situation. The coalition head has been specified with an "H". The cognitive base station has been identified by "CBS".

Chart 2
Coalition formation algorithm applied by the CBS

Input: M_{SU}, P_j^{fa}, α, N. (It is assumed that $M_{PU} = 1$)
Initialization: The default partition is a non-cooperative scenario (S_o); Compute the number of possible partitions B_n using (7) with $n = M_{SU}$; Each SU estimates γ_j and γ_j^*, and reports to the CBS the error and detection probabilities, P_j^{err} and P_j^{det}, computed using (6) and (13), respectively;
While the coalitional game is running *bestPartition* = S_o; **For** partition index $k = 1, 2, ..., B_n$ *currentPartition* = S_k; Compute the utility of each coalition in the *k*-th partition using (2)-(5); Apply the Pareto order as in (1) and compare *currentPartition* with *bestPartition*; **If** *currentPartition* is preferred over *bestPartition* *bestPartition* = *currentPartition*; **End**
End S_o = *bestPartition*; **Procedure:** Each SU estimates γ_j and γ_j^*, and reports to the CBS the error and detection probabilities P_j^{err} and P_j^{det} computed using (6) and (13), respectively.[5] **End**

The new partition $W = \{W_1, W_2\}$ in Fig. 3 (b) presents a higher utility for individual users (i.e., $W \mid> S$), according to the detection and false-alarm probabilities obtained by means of cooperation. For a more extensive analysis of secondary user's behavior under changing conditions, an SNR margin $\Delta\gamma$, in the range from -4 dB to $+8$ dB, was added to parameters γ_j and γ_j^* for every secondary user. As shown in Fig. 4, for SNRs between -12 dB and 16 dB, the best option for SU_4 is to form partition W. However, for SNRs outside this bounds, cooperation is deprecated, since it produces a poorer detection performance for SU_4. This is a consequence of the probability of error P^{err} that characterizes the reporting channel during cooperation, as expressed in (6).

[5] The coalitional game could be paused if, after updating the error and detection probabilities, they have not significantly changed. Continue the game only if a significant change has occurred, due to users' mobility, changes in the channel's statistics, etc.

In order to describe the performance of the cooperative scenario presented above under security threats, several attacks in both; the observation and the acting phase of the cognitive cycle were included in simulations. In the observation phase, Byzantine attacks were considered. In the acting phase, jamming attacks over the sensing channel was included.

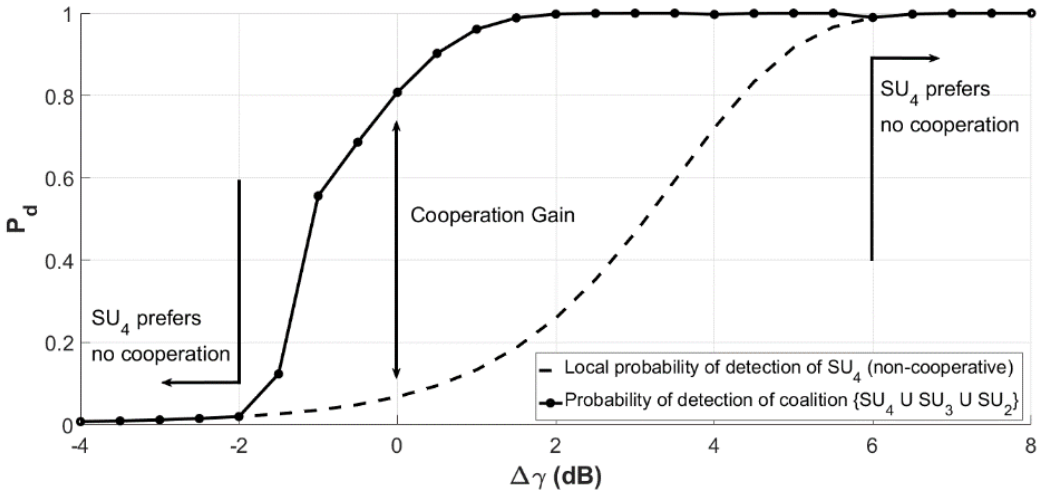

Figure 4

Probabilities of detection for the worst positioned secondary user (SU_4) under partitions S and W, respectively.

Jamming attacks over the sensing channel: one attacker transmits white Gaussian noise in order to decrease the SNR at the receivers and consequently to decrease the detection rate, as can be derived from (13). In simulations, one secondary user (SU_3) was attacked with a jamming level of 10 dB over the sensing channel.

Byzantine attacks: one secondary user inside the network intentionally sends wrong reports regarding the presence or absence of a primary user's signal. In simulations, one malicious user was included (SU_3). Let $\check{P}_j^{\text{det}}$ and $\check{P}_j^{\text{fal}}$ be the probabilities of detection and of false-alarm for the malicious user, respectively. It is easy to realize that Byzantines turn both probabilities to the complements of their equivalent for an honest user, i.e.:

$$\check{P}_j^{\text{fal}} = 1 - P_j^{\text{fal}} \tag{14}$$

$$\check{P}_j^{\text{det}} = 1 - P_j^{\text{det}} \tag{15}$$

The cognitive radio network sates have been summarized in Chart 3. Before the coalitional game started, secondary users performed local spectrum sensing, and obtained individual detection and false-alarm rates. SU_4 had a very poor detection rate of 0.068 and thus a significant interference rate $\tau_j^{\mathcal{H}_1}$ according to (9). Observe also the poor detection rate of 0.002 for SU_3 when attacked by a jammer. When SU_3 is malicious, it's detection a false-alarm rates (0.741; 0.999) are the complements of those obtained as an honest user (0.259; 0.001). However, its Byzantine attacks have no effects in other secondary users, since no cooperation is applied.

Chart 3
Cognitive radio network sates under jamming and Byzantine attacks[6]

Sate:	Conditions:			Partition selected:	Detection performance:							
					SU_1		SU_2		SU_3		SU_4	
	No attacks	Jamming attack	Byzantine attack		P_d	P_{fa}	P_d	P_{fa}	P_d	P_{fa}	P_d	P_{fa}
Before cooperation	X			$\{SU_1, SU_2, SU_3, SU_4\}$	1.000	0.001	0.721	0.001	0.259	0.001	0.068	0.001
		X		$\{SU_1, SU_2, SU_3, SU_4\}$	1.000	0.001	0.721	0.001	0.002	0.001	0.068	0.001
			X	$\{SU_1, SU_2, SU_3, SU_4\}$	1.000	0.001	0.721	0.001	0.741	0.999	0.068	0.001
After cooperation	X			$\{SU_1, SU_2 \cup SU_3 \cup SU_4\}$	1.000	0.001	0.808	0.008	0.808	0.008	0.808	0.008
		X		$\{SU_1, SU_2 \cup SU_3 \cup SU_4\}$	1.000	0.001	0.741	0.008	0.741	0.008	0.741	0.008
			X	$\{SU_1, SU_3, SU_2 \cup SU_4\}$	1.000	0.001	0.740	0.005	0.259	0.999	0.740	0.005

[6] In Chart 3, P_d and P_{fa} represent the coalitional probabilities ($Q^{\text{det}}, Q^{\text{fal}}$) perceived by a particular user in a specific coalition.

After applying the coalition formation algorithm using parameters and terms presented above, the coalitional game reaches an equilibrium in which SU_1 is a coalition itself (highlighted in green color), while SU_2, SU_3 and SU_4 form a coalition to improve their common detection rate (highlighted in blue color), as illustrated in Fig. 3 (b). When no attacks are considered, coalition W_2 shares a common detection rate of 0.808 which is beneficial for all of its members, reducing dramatically their individual interference rates and yet with a reasonable false-alarm rate under the penalty barrier α. When SU_3 is attacked by a jammer during the coalitional game, the whole coalition is affected, and the new detection rate is 0.741 for all of its members, even if two of them have not been directly attacked. On the other hand, when SU_3 acts as a Byzantine attacker, the coalitional game reaches an equilibrium in which this attacker is out of any coalition. As a matter of fact, due to its false-alarm rate higher than the penalty barrier α, this attacker is automatically out of the game. However, a Byzantine attacker might intentionally report wrong P_j^{err} and P_j^{det} estimations during the coalition formation algorithm in Chart 2, in order to achieve a lower coalitional false alarm rate. For such case, a more complex countermeasure should be considered.

6.- DISCUSSION AND FUTURE WORK

The cooperation protocol is still a challenge for practical scenarios. In this paper, the global decision that determines which partition to form, was conducted in a centralized manner. A cognitive base station computes, for every possible partition, the utilities associated with each coalition, as described in equation (2), and finally takes the optimal decision according to the comparison rule. The corresponding overhead in a centralized scheme can be significant for a greater number of users, which deteriorates the throughput of the network. A more convenient cooperation protocol must be analyzed in a future work to deal with this drawback. For the sake of simplicity, the cooperative approach described in this paper considers the existence of a common channel for secondary users to report their local spectrum sensing decision. However, in the context of cognitive radio networks, spectrum availability perceived by each secondary user might be different. Consequently, a common reporting channel for every user in the network cannot be assured. This limitation should be considered in a future work. In this research, an exhaustive search optimization was used in the coalition formation algorithm to find the optimal partition. The number of utility function evaluations increases dramatically with the number of users in the network, according to the Bell number. For a larger number of secondary users in the network, a meta-heuristic optimization method could be employed, and the number of utility function evaluation can be reduced and yet allow to find a nearly-optimal or even the optimal partition with a significantly reduced delay due to convergence. A further research in this area should be made. Only one sensing channel was considered. A single channel might not meet the traffic demand of the network. To deal with this subject, the authors in [31] propose a cooperation model with a game in which M primary users and N secondary users use the same spectrum frequencies divided into M allocated channels. Regarding security threats, only a descriptive study has been presented in this paper. Simulation results showed up remarkable security vulnerabilities that must be addressed in a deeper research. Countermeasures and methods to improve robustness must be analyzed in a future research.

7.- CONCLUSIONS

In this paper, a comprehensive study of cooperative communications for cognitive radio networks have been carried out, focusing on its main benefits and drawbacks. Moreover, a survey of applications related to cooperative communications was performed. In this regard, game theory models were presented as a reasonable approach for optimizing resources in communication systems. Coalitional games allow to deal with changing conditions in a cooperative scenario, however, some challenges summarized in this paper must be taken into account for practical applications. Security issues for wireless cognitive radio networks were analyzed for different phases of the cognitive cycle. Simulations show that coalitional games may effectively improve the efficiency in the use of the frequency spectrum, by performing dynamic coalitions formation. Simulations regarding security threats were performed too, for different kinds of attacks. Simulation results reveal that such vulnerabilities must be addressed, otherwise cooperation may be unaffordable. Further studies must be conducted to design a cognitive radio network with more practical restrictions than those included in this research.

ACKNOWLEDGMENTS

The authors are grateful to the anonymous referees who called their attention to recent work on the topic. All their suggestions helped to improve this paper. This work was partially supported by the Complex of Integrated Technological Investigations (CITI).

REFERENCES

1. Wang G, Liu Q, He R, Gao F, Tellambura C. Acquisition of channel state information in heterogeneous cloud radio access networks: challenges and research directions. IEEE Wireless Communications. 2015;22:100-7.
2. Global Mobile Data Traffic Forecast Update 2014–2019. In: CISCO VNI, editor.; February 2015.
3. Esmaeeli M, editor Improving energy efficiency using a new game theory algorithm for wireless sensor networks. International Journal of Computer Applications; 2016.
4. Kim J, Lee J, Kim J, Yun J. M2M Service Platforms: Survey, Issues, and Enabling Technologies. IEEE Communications Surveys Tutorials. 2014;16:61-76.
5. Mitola J, Maguire GQ. Cognitive radio: making software radios more personal. IEEE Personal Communications. 1999;6:13-8.
6. Baldini G, Sturman T, Biswas AR, Leschhorn R, Godor G, Street M. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead. IEEE Communications Surveys Tutorials. 2012;t14:355-79.
7. Han Z. Game Theory in Wireless and Communication Networks: Theory, Models, and Applications: Cambridge University Press; 2012.
8. Yu FR, Huang M, Tang H. Biologically inspired consensus-based spectrum sensing in mobile Ad Hoc networks with cognitive radios. IEEE Network. 2010;24:26-30.
9. Mao X, Ji H, editors. Biologically-Inspired Distributed Spectrum Access for Cognitive Radio Network. 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM); September 2010.
10. Li G, Oh SW, Teh KC, Li KH, editors. Enhanced BIOlogically-inspired Spectrum Sharing for cognitive radio networks. 2010 IEEE International Conference on Communication Systems (ICCS); November 2010.
11. Balaji V, Hota C, editors. Efficient cooperative spectrum sensing in Cognitive Radio using coalitional game model. 2014 International Conference on Contemporary Computing and Informatics (IC3I); November 2014.
12. Saad W, Han Z, Debbah M, Hjorungnes A. A distributed coalition formation framework for fair user cooperation in wireless networks. IEEE Transactions on Wireless Communications. 2009;8:4580-93.
13. Akyildiz IF, Lo BF, Balakrishnan R. Cooperative Spectrum Sensing in Cognitive Radio Networks: A Survey. Phys Commun. 2011;4:40–62.
14. Weisstein EW. CRC Concise Encyclopedia of Mathematics, Second Edition: CRC Press; 2002. 3253 p.
15. Saad W, Han Z, Debbah M, Hjorungnes A, editors. A Distributed Merge and Split Algorithm for Fair Cooperation in Wireless Networks. ICC Workshops - 2008 IEEE International Conference on Communications Workshops; May 2008.
16. Brandt R, Mochaourab R, Bengtsson M. Distributed Long-Term Base Station Clustering in Cellular Networks using Coalition Formation. IEEE Transactions on Signal and Information Processing over Networks. 2016;PP:1-.
17. Zhang N, Mark JW. Security-aware Cooperation in Cognitive Radio Networks. New York, NY: Springer New York; 2014.
18. Unnikrishnan J, Veeravalli VV. Cooperative Sensing for Primary Detection in Cognitive Radio. IEEE Journal of Selected Topics in Signal Processing. 2008;2:18-27.
19. Sharma RK, Rawat DB. Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey. IEEE Communications Surveys Tutorials. 2015;17:1023-43.
20. Attar A, Tang H, Vasilakos AV, Yu FR, Leung VCM. A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions. Proceedings of the IEEE. 2012;100:3172-86.
21. Chen L, Ji H, Li Y, Li X, editors. Distributed cooperative spectrum sensing for cognitive radio networks. 2012 IEEE Wireless Communications and Networking Conference (WCNC); April 2012.
22. Lai J, Dutkiewicz E, Liu RP, Vesilo R, editors. Comparison of cooperative spectrum sensing strategies in distributed cognitive radio networks. 2012 IEEE Global Communications Conference (GLOBECOM); December 2012.
23. Misra S, Saha BK, Pal S. Evolutionary Game in Wireless Networks. Opportunistic Mobile Networks: Springer International Publishing; 2016. p. 163-89.
24. Zhang L, Ding G, Wu Q, Zou Y, Han Z, Wang J. Byzantine Attack and Defense in Cognitive Radio Networks: A Survey. IEEE Communications Surveys Tutorials. 2015;17:1342-63.
25. Fragkiadakis AG, Tragos EZ, Askoxylakis IG. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. IEEE Communications Surveys Tutorials. 2013;15:428-45.
26. Pietro RD, Oligeri G. Jamming mitigation in cognitive radio networks. IEEE Network. 2013;27:10-5.
27. Wang B, Wu Y, Liu KJR, Clancy TC. An anti-jamming stochastic game for cognitive radio networks. IEEE Journal on Selected Areas in Communications. 2011;29:877-89.

28. Chen C, Song M, Xin C, Backens J. A game-theoretical anti-jamming scheme for cognitive radio networks. IEEE Network. 2013;27:22-7.
29. Wu Y, Wang B, Liu KJR, Clancy TC. Anti-Jamming Games in Multi-Channel Cognitive Radio Networks. IEEE Journal on Selected Areas in Communications. 2012;30:4-15.
30. Song J, Feng Z, Zhang P, Liu Z. Spectrum sensing in cognitive radios based on enhanced energy detector. IET Communications. 2012;6:805-9.
31. Moualeu JM, Ngatched TMN, Hamouda W, Takawira F, editors. Energy-efficient cooperative spectrum sensing and transmission in multi-channel cognitive radio networks. 2014 IEEE International Conference on Communications (ICC); June 2014.
32. Eryigit S, Bayhan S, Tugcu T. Energy-Efficient Multichannel Cooperative Sensing Scheduling With Heterogeneous Channel Conditions for Cognitive Radio Networks. IEEE Transactions on Vehicular Technology. 2013;62:2690-9.
33. Ma X, Zeng F, Xu J, editors. A novel energy efficient cooperative spectrum sensing scheme for cognitive radio sensor network based on evolutionary game. 2015 IEEE International Workshop on Local and Metropolitan Area Networks (LANMAN); April 2015.
34. Hu H, Zhang H, Yu H, Chen Y. Spectrum-energy-efficient sensing with novel frame structure in cognitive radio networks. AEU - International Journal of Electronics and Communications. 2014;68:1065-72.
35. Tandra R, Sahai A. SNR Walls for Signal Detection. IEEE Journal of Selected Topics in Signal Processing. 2008;2:4-17.

AUTHORS

Luis Miguel Gato Díaz, Engineer on Telecommunications and Electronics, Department of Telecommunications and Telematics, Technological University of Havana (CUJAE), Cuba, luis.gd@tele.cujae.edu.cu. His research interests include cognitive radio networks, cooperative communications, and wireless physical-layer security for the next-generation communication systems.

Meiby Ortiz Bouza, Senior student on Telecommunications and Electronics Engineering, Technological University of Havana (CUJAE), Cuba, mortizb@fecrd.cujae.edu.cu. Her areas of research include cognitive radio networks and cooperative communications.

Jorge Torres Gómez, Engineer on Telecommunications and Electronics, Ph.D., Department of Telecommunications and Telematics, Technological University of Havana (CUJAE), Cuba, jorge.tg@tele.cujae.edu.cu. His research interests include digital signal processing, cognitive radio networks and software defined radio.