Misbehaviour detection in Cognitive and Cooperative Networks

Lorenza Giupponi and Christian Ibars
Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)
Av. Canal Olímpic s/n 08860
Castelldefels (Barcelona), Spain
Email: [lorenza.giupponi,christian.ibars]@cttc.es

Abstract—This paper presents an approach to detect misbehaving nodes in cognitive and cooperative networks. In particular, we propose a cooperative scheme, where cognitive radios are granted access in licensed bands, as long as they compensate primary (licensed) users for the additional interference generated in their bands through cooperation. However, this cooperative transmission can be vulnerable to malicious attacks, which are not easy to detect, since they may affect the error probability experienced by the primary users, but not their signal to noise and interference ratio. We propose a misbehaviour detection approach based on measuring and comparing the entropy of data derived by anomalous and normal behaviors. Simulation results show that the probability of detection strongly depends on the transmission power and spectrum handoff rate of the outliers.

I. INTRODUCTION

Cognitive Radio is a new paradigm in wireless communications to enhance utilization of limited spectrum resources. It is defined as a radio able to utilize available side information, in a decentralized fashion, in order to efficiently use the radio spectrum left unused by licensed systems. The basic idea is that a secondary (unlicensed) user (SU) is able to properly sense the spectrum conditions and, to increase efficiency in spectrum utilization, it seeks to underlay, overlay or interweave its signals with those of the primary (licensed) users (PUs), without impacting their transmission [1]. Many contributions can be encountered in literature showing that all the challenges related to the so called cognitive radio cycle [2] can highly benefit from cooperation, not only among SUs [3], [4], but also between SUs and PUs. This implies that SUs may act as relays of the primary signals, which creates sever consequences in terms of security and feasibility. This is the motivation of this paper, since, to the best of the authors’ knowledge, little work can be found in literature about this problem [5]. As a result, in this paper we consider one of the cooperative approaches for cognitive radios presented in literature, an we improve it against node misbehavior. In particular, in [6], the authors present a cooperative scheme where concurrent primary and secondary communications are allowed by exploiting spatial reuse, as long as the SUs cooperate with the PUs active in the same frequency channels. SUs cooperate by relaying the primary messages to their final destination. The objective is to improve the performances of the PUs and to compensate them for the increased interference at their receivers. A game theoretic framework based on the theory of Bayesian potential games is proposed to model power and channel allocation in a cognitive radio scenario where the individual decisions of SUs strongly depend on the decisions made by the SUs. In fact, the PUs’ performances are limited by the aggregated interference generated by all the SUs simultaneously transmitting in their band. The hypothesis of incomplete information was considered in the decision making process, so as to avoid the need for a Common Control Channel (CCC), where users share information.

Such a cooperative scheme can suffer from various attacks since secondary users have the chance to act as relays of the primary communications, and instead of forwarding correct information, they might send arbitrary information to the primary destination, thus significantly damaging the primary system performance. However, these behaviors are difficult to detect, since they do not affect the received signal to noise and interference ratio (SINR), but may significantly increase the error probability of the communication, which, on the other hand, may also be affected by multiple factors, e.g. noise, interference and adverse channel condition, in general unknown to the destination node. A frequently proposed solution to node misbehavior in decentralized networks is to use reputation systems, where each node is associated with a certain value of node-centric trust/reputation derived via fairly lengthy interactions among nodes, which keep track of past behaviors. However, in cognitive radio networks, it is infeasible to monitor the neighbors’ behavior during a long enough time, since nodes are characterized by high spectral mobility and switch from one frequency channel to another, through the operation of spectrum handoff [2]. Consequently, the interactions among primary and secondary users are in general quite transient and do not rely on any prior association, so that traditional trust schemes cannot be directly applied.

In such scenarios, it is more useful to establish trust in data, rather than in the nodes who generated them. In this paper, we take as a basis the game theoretic scheme proposed in [6] and we propose a data-centric approach to detect misbehavior in cognitive radio networks based on cooperation among secondary and primary users. In particular, we propose to detect data anomalies by monitoring specific metrics related to error probability, comparing the actual metric values to the expected values, and thresholding their deviation. We use the concept
of entropy, a typical measure of information, which provides an adaptive solution capable of building data models on the fly to represent anomalous and normal behaviors of error probability and then compare them. The outline of the paper is organized as follows. Section II describes the system model. Section III presents the game theoretic model for power and channel allocation in an environment with partial information, and discusses the existence of a Bayesian Nash equilibrium. In particular, cooperation among PUs and SUs is modeled through a game where the SUs are the players and among their actions they may choose to either act cooperatively, or misbehave. In case of misbehavior, Section IV presents a strategy for detecting it. Section V describes the simulation scenario where the proposed approach is evaluated. Section VI is devoted to the discussion of representative simulation results. Finally, Section VII summarizes the conclusions of the paper.

II. SYSTEM MODEL

The cognitive radio network we consider consists of \( M \) transmitting-receiving PUs pairs, and \( N \) transmitting-receiving SUs pairs. In this paper we will indicate the transmission power levels of the PUs' transmitters as \( p_i^P \), \( i = 1, \ldots, M \), and the transmission power levels of the SUs' transmitters as \( p_j^S \), \( j = 1, \ldots, N \). PUs and SUs, both transmitters and receivers, are randomly and uniformly distributed in a circular coverage region of a primary network with radius \( R_{\text{max}} \). Primary communications can be characterized by a long distance between the transmitting and the receiving device, whereas secondary communications are in general characterized by short range. The nodes are either fixed, or are moving slowly (slower than the convergence of the proposed game). A SU distributively selects the frequency channel, among \( l \) available, and the transmission power level, among \( m \) available, in order to maximize its throughput while at the same time not causing harmful interference to the PUs. Besides, the SUs have to compensate the PUs for using their frequency band; they do so by devoting part of their transmission power to relaying the primary transmission.

We consider that the secondary users are either correct, i.e. they comply with the cooperative behavior, or they deviate from the cooperative scheme, intentionally (i.e. they are attackers) or unintentionally (i.e. they are faulty nodes). Both the attackers and the faulty nodes can cause damage to the primary system and hence we consider both of them as adversaries. We consider that both correct and adversary secondary users are players of the game defined in section III, so that they select their frequency channel and transmission power level, based on the same utility function. Besides, among their strategies, they choose to either cooperatively behave, or misbehave. In this case, the adversary nodes send garbage information to the primary receiver when they serve as relays. This information is processed by the PU receiver and degrades its ability to correctly detect the received signal. In addition, it may be difficult to detect since it follows the PU signal format.

The cooperative scheme used by the SUs is shown in Fig. 1. We assume that the PU transmission is divided into frames, and each frame further into slots. Relays are assumed to operate in half-duplex mode. Therefore, each relay listens to the primary transmission during one slot and transmits during the next. The relay will choose, as part of its strategy, whether to listen during even or odd slots. We consider D&F relaying technique, where the relay (secondary user) decodes the primary signal, regenerates it and retransmits it during the next time slot. In the event that the relay is unable to decode, then it remains silent. We define the two slot subsets as \( S_1 \) and \( S_2 \) respectively. To support the cooperative relaying scheme, a PU receiver technique suitable for space-time coding is assumed.

As for the transmission power level \( p_j^S \), allocated to SU \( j \), a benign SU splits it in two parts, 1) a power level \( p_j^{S'} \), \( j = 1, \ldots, N \) for its own transmission, 2) a cooperation power level \( p_j^{S''} \), \( j = 1, \ldots, N \), for relaying the PU’s message on the selected band, where \( p_j^S = p_j^{S'} + p_j^{S''} \). In turn, if the SU is malicious, part of its transmission power is devoted to relaying a primary message, after having arbitrarily modified its content. In this case, the power level allocated for malicious use is indicated with \( p_j^{S'''} \), so that \( p_j^S = p_j^{S'} + p_j^{S'''} \). To sum up, when a SU is correctly cooperating, \( p_j^{S''} \neq 0 \) and \( p_j^{S'''} = 0 \). In turn, when a SU is acting maliciously, \( p_j^{S''} = 0 \) and \( p_j^{S'''} \neq 0 \). We shall analyze the network performance in terms of SINR of both PUs and SUs and outage probability. As for the notation, we indicate with \( h_{ij}^{PP} \) the link gain between a PU’s transmitter \( i \) and a PU’s receiver \( j \); with \( h_{ij}^{PS} \) the link gain between a PU’s transmitter \( i \) and a SU’s receiver \( j \); with \( h_{ij}^{SP} \) the link gain between a SU’s transmitter \( i \) and a SU’s receiver \( j \); with \( h_{ij}^{SS} \) the link gain between a SU’s transmitter \( i \) and a SU’s receiver \( j \). \( \sigma^2 \) is the noise power (assumed to be the same in each channel).

In addition, we will use the notation \( s_l \) to refer to the slot subset chosen by SU \( i \), and we define the function \( f' \)

\[
  f'(s_l, s_j) = \begin{cases} 
  1 & \text{if } s_l = s_j \\
  0 & \text{if } s_l \neq s_j 
  \end{cases} 
\]

In the D&F approach, the SU must be able to correctly decode the primary signal to relay it. In order to do that, the SINR of
the primary signal at SU transmitter \( i \), which is given by

\[
\gamma_i^{PS} = \frac{p_i^P h_{ji}^{PS}}{\sigma^2 + \sum_{k=1, k \neq i}^{N} p_k^S h_{ki}^{SS} f(c_k, c_i) f'(s_k, s_i)},
\]

where \( i = 1, \ldots, N \) must be above the sensitivity threshold, \( \rho \). In the equation, we use \( h_{ji} \) and \( h_{ki} \) to denote the channel gains to the SU transmitter, rather than the SU receiver, of SU pair \( i \). We define the function

\[
f''(\gamma_i^{PS} > \rho) \equiv \begin{cases} 1 \text{ if } \gamma_i^{PS} > \rho \\ 0 \text{ otherwise} \end{cases}
\]

The SINR of the PU \( i \) will be time-varying on the two slot subsets \( S_i \), \( i \in \{1, 2\} \), and in the absence of any attack is given by:

\[
\gamma_i^{PU}(S_i) = \frac{p_i^P h_{ji}^{PS} \sum_{j=1}^{N} g_{ji}^i h_{ji}^{SS} f(c_j, c_i) f'(s_l, s_i) f''(\gamma_i^{PS} > \rho)}{\sum_{j=1}^{N} g_{ji}^i h_{ji}^{SS} f(c_j, c_i) f'(s_l, s_i) + \sigma^2},
\]

\( i = 1, \ldots, M \)

As a conservative choice, in our performance evaluation we consider the minimum SINR in any of the two slot subsets, as it normally dominates the error rate.

### III. Game Formulation and Bayesian Nash Equilibrium Existence

Game theory constitutes a set of mathematical tools to analyze interactions in decision making processes. In this paper we model joint channel and transmission power selection for cognitive radios with incomplete information as the output of a Bayesian Potential game. In particular, the considered game of incomplete information is defined as: \( \Gamma = \{ N; \{ S_i \}_{i \in N}, \{ \eta_i \}_{i \in N}, \{ f_{H_i}(\eta_i) \}_{i \in N}, \{ u_i \}_{i \in N} \} \), where:

- \( N \) is the finite set of players, i.e. the SUs. Additionally, \( N^+ \) is a finite set with \( N^+ \supseteq N \) and \( N^+ \setminus N \) is the set of outside players (i.e. the PUs).
- \( i \) For every \( i \in N, S_i \) is the set of strategies of player \( i \).

More in particular they are:

- a power level \( p_i^S \) in the set of power levels \( PS = \{ p_i^S, \ldots, p_m^S \} \);
- the power level \( p_i^{S'} \) that the player devotes to its own transmissions, in the set of power levels \( PS' = \{ p_1^{S'}, \ldots, p_q^{S'} \} \), where \( q \) is the order of set \( PS' \);
- the cooperative power level \( p_i^{S''} \) that the player, in case of benign behavior, devotes to relaying a PU transmission and which is computed as \( p_i^{S''} = p_i^S - p_i^{S'} \). The set of these power levels, \( PS'' \), is the same as \( PS' \);
- the malicious power level \( p_i^{S'''} \) that the player, in case of malicious behavior, devotes to relaying a PU transmission and which is computed as \( p_i^{S'''} = p_i^S - p_i^{S''} \). The set of these power levels, \( PS''' \), is the same as \( PS'' \);
- a channel \( c_i \) in the set of channels \( C = \{ c_1, \ldots, c_t \} \);
- a slot subset \( s_l \) from the two possible subsets \( S_1 \) (even) and \( S_2 \) (odd).

These strategies can be combined into a composite strategy \( s_i = (p_i^S, p_i^{S'}, p_i^{S''}, p_i^{S'''}, c_i, s_l) \in S_i \). We define \( S = \times S_i, i \in N \) as the strategy space.

\( iii \) A game of incomplete information, with respect to a game of complete information, is characterized by the player’s type, which embodies any information that is not common knowledge to all players and is relevant to the players’ decision making. This may include the player’s utility function, his belief about other player’s utility functions, etc. For every \( i \in N^+, H_i \) is the finite set of possible types of player \( i \), \( \eta_i = (h_{i_1}^{SS}, \ldots, h_{i_{N+1}}^{SS}, h_{i_{N+2}}^{SS}, \ldots, h_{i_N}^{SS}) \in H_i \), which includes the wireless channel gains of player \( i \). Each player is assumed to observe perfectly its type, but is unable to observe the types of its neighbors.

\( iv \) \( f_{H_i}(\eta_i) \) is a probability distribution on \( H = \times H_i, i = 1, \ldots, N \), with the a priori probability density function (PDF) on \( H \) defining the wireless channel gain PDF.

\( v \) For every \( i \in N, u_i : S \times H \rightarrow \mathbb{R} \) is the utility function of player \( i \).

The utility function for player \( i \) is a function of its realized channel gains \( \eta_i \in H_i \) and its chosen strategy \( s_i \in S_i \), as well as the channel gains of the other SUs and PUs (i.e. \( \eta_{-i} \)) and the strategies of other players (\( s_{-i} \)).

\[
\begin{align*}
u(s_i, s_{-i}; \eta_i, \eta_{-i}) &= - \sum_{j=1}^{M} p_j^S h_{ij}^{PS} f(c_i, c_j) \\
&- \sum_{j=1, j \neq i}^{N} p_j^S h_{ij}^{SS} f(c_j, c_i) f'(s_l, s_i) \\
&- \sum_{j=1, j \neq i}^{N} p_j^S h_{ij}^{SS} f(c_i, c_j) f'(s_l, s_j) \\
&+ b \log(1 + p_i^{S'} h_{ij}^{SS}) + \alpha_i \sum_{j=1}^{M} p_j^{S''} h_{ij}^{SP} f(c_i, c_j) f''(\gamma_i^{PS} > \rho) \\
&+ (1 - \alpha_i) \sum_{j=1}^{M} p_j^{S'''} h_{ij}^{SP} f(c_i, c_j) f''(\gamma_i^{PS} > \rho)
\end{align*}
\]

where \( \alpha_i \) indicates if the secondary user \( i \) is acting maliciously (\( \alpha_i=1 \)) or not (\( \alpha_i=0 \)). The expression presented in (5) consists of six terms. The first and the third terms account for the interference perceived by the PUs and by the other SUs in \( c_i \) (and \( s_l \) for the SUs) from player \( i \), which only consists of the power the user \( i \) devotes to the secondary transmission (i.e. \( p_i^S \)). The second term accounts for the interference generated by the SUs active in channel \( c_i \) and slot \( s_l \) on player \( i \). The fourth term represents an incentive for the individual players to increase the power level devoted to their own communications. We weight this term by a coefficient \( b \) to give it more or less importance than the other terms of the utility function. The fifth term, is a positive contribution to the utility function and accounts for the benefit provided to the PUs by the relaying realized by the SUs. This term is positively defined to encourage SUs to cooperate with PUs in exchange for using their frequency channel. In case the
secondary user is malicious, it allocates a cooperative power equal to zero and a malicious power $p_i^{S''}$, which generates a positive contribution to the utility function (the sixth term), to indicate the satisfaction of the secondary user for realizing a malicious attack.

It can be easily demonstrated that the game $\Gamma$, with utility function defined in (5), is a Bayesian Potential game [6]. Specifically, a Bayesian game is Potential if there exists a function $\text{Pot} : S \rightarrow \mathbb{R}$ such that, for all $i \in N$, $s_i, s_i' \in S_i$ and $\eta_i, \eta_{-i} \in \mathcal{H}$:

$$\text{Pot}(s_i, s_{-i}; \eta_i, \eta_{-i}) - \text{Pot}(s_i', s_{-i}; \eta_i, \eta_{-i}) = u(s_i, s_{-i}; \eta_i, \eta_{-i})$$

(6)

The function $\text{Pot}$ is called exact potential function of the game $\Gamma$ and it reflects the change in utility for any unilaterally deviating player. For the previously defined game we can define the potential function defined in (7).

$$\text{Pot}(s_i, s_{-i}; \eta_i, \eta_{-i}) = \sum_{i=1}^{N} \left( \sum_{j=1}^{M} -p_i^{SP} h_{ij}^{SP} f(c_i, c_j) \right)$$

$$+ \sum_{i=1}^{N} \left( -a \sum_{j=1, j\neq i}^{N} p_i^{SP} h_{ij}^{SS} f(c_i, c_j) f'(s_lj, s_{lj}) \right)$$

$$+ \sum_{i=1}^{N} b \log(1 + p_i^{SP} h_{ii}^{SS})$$

$$+ \sum_{j=1}^{M} (p_j^{S''} + p_j^{S'''} h_{ij}^{SP} f(c_i, c_j) f''(\gamma_{PS} > \rho)$$

(7)

The players make decisions in a decentralized fashion, and independently, but they are influenced by the other players’ decisions. In this context, we are interested in searching an equilibrium point for the joint power and channel selection problem of the SUs from which no player has anything to gain by unilaterally deviating. This equilibrium point, in games of complete information, is known as Nash equilibrium. We define a Bayesian Nash equilibrium as a Nash equilibrium of a Bayesian game. In particular, a strategy profile $s^* = (s_1^*, ..., s_N^*)$ is a Bayesian Nash equilibrium if $s_i^*(\eta_i)$ solves (8), assuming that types of different players are independent.

$$s_i^*(\eta_i) = \arg\max_{s_i \in S_i} \sum_{\eta_{-i}} f_H(\eta_{-i}) u_i(s_i, s_{-i}; \eta_i, \eta_{-i})$$

(8)

As it is proven in [7], the existence of a Bayesian Nash equilibrium is an immediate consequence of the Nash existence theorem. As a result, considering that the potential games have shown to always converge to a Nash Equilibrium when a best response adaptive strategy is applied, it can be derived that for the Bayesian Potential game $\Gamma$ there exists a Bayesian Nash equilibrium, which maximizes the expected utility function defined in (5).

IV. MISBEHAVIOR DETECTION

In a cognitive radio system where the PU can grant or deny access to the band by SUs, we are interested in providing a mechanism for the PU to detect misbehavior and then take action correspondingly. The behavior of malicious SUs is defined by their utility function, described in Section III. They send a malicious signal with power $p_j^{S'''}$. The malicious signal is taken by the primary as benign and incorporated in the detection process. It also contributes positively to the calculation of the received SINR, which is assumed to be done in the header field. However, the malicious signal disrupts the detection process and increases the received error probability.

The proposed misbehavior mechanism relies on detecting whether the error probability of the received signal is higher than what corresponds to the received SINR. In order to do that, we rely on an error detection mechanism that is able to detect the number of errors in a given frame. The received SINR of the PU in the event of an attack is given by:

$$\gamma_i^{PU_{at}}(S_i) = \frac{p_i^{SP} h_{ii}^{PP} \sum_{j=1}^{N} p_j^{S''} \gamma_{PS}^{SP}(s_lj, s_{lj}) f''(\gamma_{PS} > \rho)}{\sum_{j=1}^{N} (p_j^{S'''} + p_j^{S'''} h_{ij}^{SP}) f'(s_lj, s_{lj}) f''(\gamma_{PS} > \rho) + \sigma^2}$$

i = 1, ..., M

This SINR value will yield the actual error probability on the received frame. Furthermore, the apparent SINR of the PU (calculated from the header field) is given by:

$$\gamma_i^{PU_{ap}}(S_i) = \frac{p_i^{SP} h_{ii}^{PP} + \sum_{j=1}^{N} (p_j^{S'''} + p_j^{S'''} h_{ij}^{SP}) f'(s_lj, s_{lj}) f''(\gamma_{PS} > \rho)}{\sum_{j=1}^{N} (p_j^{S'''} + p_j^{S'''} h_{ij}^{SP}) f'(s_lj, s_{lj}) f''(\gamma_{PS} > \rho) + \sigma^2}$$

i = 1, ..., M

This SINR value will yield an expected error probability lower than the actual measured one.

For the sake of simplicity, we assume that the transmitted signal uses BPSK (Binary Phase Shift Keying) modulation. Furthermore, we assume that interference at the receiver can be approximated as Gaussian. Under these assumptions, the error probability for PU $i$ is given by:

$$P_e = Q \left( \sqrt{\gamma_{i}^{PU_{ap}}} \right)$$

(11)

where $Q(x)$ is the Gaussian right tail integral,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-t^2/2} dt$$

(12)

Note that the results can be easily generalized to higher modulation orders by using the appropriate error probability function.

In order to detect the attack, we wish to compare the error probability $P_e$, which can be expected from the measured SINR $\gamma_{i}^{PU_{ap}}$, with the actual error probability, generated by SINR $\gamma_{i}^{PU_{at}}$. We do so by comparing the distribution of $P_e$ to the distribution of the number of errors in each received frame, or, equivalently, the error probability within a frame.
First, for the actual error probability $\hat{P}_e$, we build a histogram of the received frame errors (which we assume is possible through the error detection mechanism). Second, for the expected error probability $P_e$, the number of errors in a frame will follow a binomial distribution

$$Pr(K = k) = \binom{N_f}{k} P^k_e (1 - P_e)^{N_f - k}$$

(13)

where $N_f$ indicates the frame size. The receiver can compare the expected probability mass function (PMF) of $P_e$, with the histogram of the received bit errors, in order to detect whether such distribution is being followed. In order to measure the distance between the two probability distributions, $p$ and $q$ we propose to use the Kullback-Leibler distance [8], defined as:

$$D(p||q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)}$$

(14)

Then, we set a threshold, and decide that an attack is underway if the distance between expected and actual error probability distributions exceeds it:

$$D(f_{PE}||f_{\hat{PE}}) > \Lambda$$

(15)

where $f_{PE}$ and $f_{\hat{PE}}$ indicate, respectively, the PMF of the expected and actual error probabilities. While this method allows to detect an attack, it does not allow the identification of the malicious users. Therefore, the likely outcome of a misbehavior detection is to ban the usage of the licensed band to all secondary users. This means that the threshold has to be carefully chosen so as to provide a good tradeoff between detection probability of an attack and false alarm probability. Furthermore, the detection probability depends on the number of frames $L$ under consideration in the histogram.

V. SIMULATION SCENARIO

The scenario considered to evaluate the proposed framework consists of a circular area with radius $R_{\text{max}} = 150$ mt. With respect to the strategy space, the set of power levels $P^S = (p^S_1, \ldots, p^S_m)$ is defined as $P^S = (0, 5, 10, 15, 20)$ dBm, i.e. $m = 5$. On the other hand, the SUs can be scheduled over $l = 4$ available frequency channels, so that the set of channels $C = (c_1, \ldots, c_l)$ is defined as $C = (1, 2, 3, 4)$. We consider $M=4$ PUs pairs, one pair for each frequency channel, and $N$ SUs pairs, which at simulation start are randomly distributed over the $l$ frequency channels. The PUs pairs are randomly located in the scenario. Specifically, the maximum distance between a PU transmitter and a PU receiver is randomly selected depending on their random position in the coverage area. On the other hand, the maximum distance between a SU transmitter and receiver is 20 mt. We consider a simplified wireless channel model, $h_{ii} = \left( \frac{10}{d_{ii}^6} \right)$, where $d_{ii}$ is the distance from transmitter $i$ to receiver $i$. The reason is that the performance of the proposed misbehavior detection scheme does not depend on it. The transmission power of a PU is 20 dBm. In order to define the PDF of the wireless channel gains, we proceed by simulations. We discretize the random variable $\tilde{R}$ representing the distance between two nodes, and accordingly the possible values of wireless channel gains, into $T$ equally spaced values. In this way we generate a path loss probability mass function (PMF) of the wireless channel gains, which is represented in Fig. 2.

VI. DISCUSSION AND RESULTS

In this section we show the impact that the different parameters of the game and of the misbehavior detection algorithm have over the detection and false alarm probabilities. First of all, the parameter $b$ defined in the utility of the game (Eq. 5) has a significant impact on the performances of the misbehavior detection algorithm. In fact, this parameter represents an incentive for the players to increase the power they devote to their secondary transmission, with respect to the cooperation/malicious power. More in particular, lower values of $b$, result in higher values of cooperative and malicious power for both correct and misbehaving players. Consequently, the malicious users attack with high power, so causing a
much stronger impact on the error probability with respect to a situation characterized by lower malicious power, which results in a more easily detectable attack. Contrarily, for higher values of $b$, the malicious players are encouraged to devote a higher percentage of their power to transmit the secondary communication, so that a lower amount of power is devoted to relaying malicious information. In this situation, the error probability at the primary receiver is less jeopardized, so that it is more difficult to detect the presence of an attack. These considerations are summarized in Fig. 3, where the probability of detection is shown with respect to the probability of false alarm, for different percentages of attackers, over the total number of SUs in the scenario. Notice that, the detection probability improves with the number of misbehaving nodes, which reduces the possibility of collusion. In addition to that, Fig. 4 shows the impact of the number of frames $L$ under consideration in the histogram, over the detection probability. It can be observed that by increasing $L$ the performances of the detection approach improve. In particular, low values of $L$ (i.e. $L=100$) can seriously jeopardize the performances of the detection algorithm. Finally, Fig. 5 describes the impact of the SUs’ spectrum mobility, in terms of the spectrum handoff rate, where the spectrum handoff rate is defined as the probability that a SU changes the frequency channel where it is operating. The dispersion of malicious users over the available channels makes more difficult the detection of the attacks, since the malicious information is spread over the different channels, so affecting less intensively multiple PU receivers.

VII. Conclusion

In this paper we have presented a misbehaviour detection algorithm to improve the security of a cooperative scheme proposed for cognitive radio networks where cognitive radios are granted access in licensed bands as long as they agree on cooperating with the primary system. The cooperative scheme was modeled by means of a Bayesian potential game where correct and misbehaving SUs are characterized by the same utility function. Misbehaving nodes attack by arbitrarily modifying the primary messages. This attack is difficult to be detected since the received SINR is not affected. In turn, the malicious signals disrupt the detection process and increase the received error probability. The proposal relies on the Kullback-Leibler distance to measure the likelihood of data models under anomalous and normal conditions. Simulation results, show that the proposed approach allows to detect anomalous behaviors of cognitive radios, and that its performances in terms of detection and false alarm probabilities strictly depend on the utility of cognitive radios, the transmission power they select through the game, the number of frames under consideration in the histogram and the secondary spectrum handoff rate.

REFERENCES