Reputation-Based Spectrum Data Fusion against Falsification Attacks in Cognitive Networks

Alessandro Galeazzi
Department of Information Engineering
University of Brescia
Brescia, Italy
a.galeazzi002@unibs.it

Leonardo Badia
Department of Information Engineering
University of Padova
Padova, Italy
leonardo.badia@unipd.it

Shi-Chung Chang
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
scchangee@ntu.edu.tw

Francesco Gringoli
Department of Information Engineering
University of Brescia
Brescia, Italy
francesco.gringoli@unibs.it

***Abstract*—The cognitive radio network paradigm increases spectrum usage efficiency by allowing secondary users to perform shared access to licensed spectrum. This systematic improvement may be obtained in a practical way by implementing a distributed cooperative spectrum sensing mechanism. Although such decentralized sensing offers many advantages, it also opens the door to new security threats such as spectrum sensing data falsification attacks. In this work, we design a new mechanism that exploits sensing correlation through the concept of reputation to enhance resilience against this type of threat. By both theoretical analysis and simulations, we show that our proposal provides incentives for cooperation among honest devices and reduces the spectrum occupancy assessment error rate in the presence of malicious users.**

I. Introduction

Over the past 20 years, the number of devices connected to the Internet has been soaring and it is predicted that the full implementation of the Internet-of-things paradigm will boost the connectivity demand [1]. Thus, a more efficient resource allocation is required to provide connection to a massive number of devices, especially in terms of spectrum usage [2]. Since the current static allocation of spectrum resources leads to low efficiency and utilization [3], [4], many regulatory bodies introduced the idea of spectrum sharing to mitigate this problem [5]. In this scenario, among the approaches proposed to detect Primary User transmission, it has been proven that the distributed sensing paradigm with the joint participation of all opportunistic users can effectively improve the system detection capability and solve sensing problems found in centralized approaches [4], but a new security threat, called Spectrum Sensing Data Falsification (SSDF), may arise [2], [6]. In this paper, we propose and analyze the performance of a novel approach to ensure the security of a CRN against SSDF attack. Our proposal is based on a reputation mechanism strengthened by channel correlation among devices. We show that our technique is able to enhance system security as long as the individual channel measures of the secondary users are sufficiently correlated. This claim is backed up by both a thorough analysis grounded in a game theory framework, where we consider the subgame perfect equilibrium of a dynamic game with infinitely many stages of reputation, as well as extensive numerical evaluations obtained via simulation.

II. Related work

The problems of a distributed sensing approach comprise two levels. First, even purely collaborative users may have an incentive for selfish behavior, i.e., an aggressive/exaggerate demand of resources by some users may lead to an increased reward for them, which is to be avoided by the network acting as a whole. Moreover, MSUs may be present in the network, and their identification is key to prevent SSDF attacks. Some strategies have been proposed to counteract both problems. In [7], it is shown how channel spatial correlation can be exploited to identify MSUs through a low rank matrix completion algorithm through an iterative procedure that identifies and disqualifies malicious users, but a rank estimation algorithm and an estimation strategy for the number of corrupted channels are required. In [8] an estimator based on beta distribution is proposed to generate a trust aware decision mechanism, but the existence of a Primary User Base Station (PUBS) in addition to the FC is supposed and communications between PUBS and FC are possible and indeed necessary. The authors of [9] analyze how the presence of MSUs can interfere with the decision made by the FC and propose a mechanism for MSU identification based on sensing time sequences and decision results. The authors of [4] stress instead how the concepts of trust and reputation are fundamental for implementing a security mechanism against SSDF attacks. By exploiting correlations on sensed data, they suggest to increase or decrease the reputation of a SU in order to assess the amount of resources assigned to a device for incentivizing honest SUs cooperation.

III. Mechanism Description and Formulation

A. *Scenario Assumption*

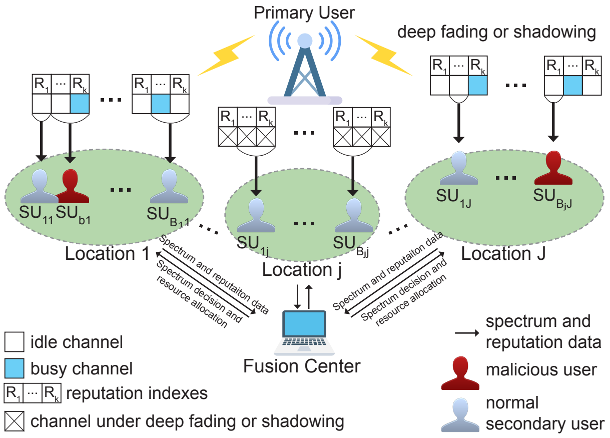


Fig. 1: Considered Scenario

In this paper, we consider the CRN system in Fig. 1 and described in the IEEE 802.22 specifications as well as the general literature on wireless transmission [7]–[13]. This scenario involves 3 entities: one primary or incumbent user, a fusion center, and a set of secondary users that have CRN capabilities. As visible from the figure, channels are directly sensed by the secondary nodes, who report to the FC both their perceived channel occupancy and a reputation about the others. The FC, in turn, aggregates these reports and makes relevant assignments. Such a model will be analyzed through the tenets of game theory, which is common in this cognitive setup.

We assume the presence of one Primary User (PU) that owns the license to access the spectrum band B. We consider N channels in the band B and a PU that can transmit through any of them at any time. The PU shares band B with other users but has a priority over other CR users in accessing spectrum band B. We now make some assumption about PUs:

- Other entities in the CRN have no specific information and details about PU transmission activities such as PU type, its transmission equipment, its transmission waveform, its location, and so on.
- The PU is transmitting from time to time, without any predefined pattern and without signaling its transmission episode to the CRN

The distributed sensing reported by the secondary users is combined through a fusion rule at the FC so as to determine the final evaluation on individual channel occupancy [9], [10], [13]. The FC is also responsible for the CR users allocation in the channels unused by PU. Further, as in [7], we assume the FC capable of splitting all the SUs into subsets based on their positions. A subset of SUs is also called a *location*. FC periodically sends to individual SUs information about which other secondary terminals are their neighbors. For each location, FC requests periodically each SUs in the location to provide data about spectrum occupancy and the SU's assessment of neighbors' reputation. Then, FC fuses SU data and makes a decision about occupancy according to a fusion rule for each channel over a location. Finally, FC assigns the available resources to SUs. We make the following assumption on the FC:

- The FC does not have any role in channel sensing. The sensing system does not rely on a central/privileged unit to sense the spectrum.

Secondary users (SUs) are unlicensed CR users that exploit the spectrum holes left by PU to access one or more of the N channels of band B. There can be two types of them: honest secondary users (HSU) and malicious secondary users (MSU) [9], [10], [13]. It is possible to distinguish between cases where all the MSUs are acting independently, or when they collaborate towards a common malicious goal; the latter would be the case where a single attacker has gained access to a set of nodes that were initially honest and corrupted them. In this paper, we consider this situation of coordinated attacks, which is clearly a worst-case scenario; clearly, our proposal works even in the case that attacks are not orchestrated by a single entity. We also make some assumptions on the sensing capabilities of cognitive terminals, namely, we assume that both HSUs and MSUs are the same type of devices, and have the same sensing capabilities. We assume that:

- A SU can identify the presence of PU and modify their transceiver parameters to exploit spectrum holes left by PU.
- For each subset of devices, the sensing measurements are strongly correlated. This implies that devices belonging to the same subset have a high probability to sense the same spectrum condition [7].
- When a SU is transmitting its spectrum and reputation data to the FC, all the devices in the same subset are able to listen and correctly decode its transmission.
- Each SU can assign a reputation index as a numerical value between 0 and 1 to all other SUs belonging to the same location. In game-theoretic terms, this value represents the *belief* that an HSU has about the other player being honest; however, MSUs are aware of their status of malicious nodes and therefore can falsify their belief too.

We now define some notation that will be useful for the next sections. In particular, we have:

$$g_{i,j} \equiv \text{Probability that SU } j \text{ is honest according to SU } i, \quad \text{where SU } i \text{ and } j \text{ are in the same location.} \tag{1}$$

Different SUs can have different indexes depending on many factor such as what they sensed or if they are MSU or HSU. We define $g_{i,i} = 0$, since in our model the self-judgment of users is not relevant. Suppose we have k SUs belonging to the same location. For each user i, we define the following vector

$$\mathbf{g}_i = [g_{i,1}, g_{i,2}, \ldots, g_{i,i-1}, 0, g_{i,i+1}, \ldots, g_{i,k}]. \tag{2}$$

Thus, $\mathbf{g}_i$ is a real vector of length K with each entry in $[0, 1]$. We now clarify the difference between HSUs and MSUs.

We suppose that both HSUs and MSUs use some energy detection techniques to assess channel occupancy. However, HSUs are ordinary devices that aim at maximizing their individual spectrum-time access and report true information to FC. Thus, we suppose HSUs do not alter spectrum reports, but they can manipulate reputation indexes to obtain more resources. This assumption is justified since an HSU aims to increase its communication opportunities and thus has no incentive for inducing a wrong decisions at the FC by altering its spectrum reports. Conversely, MSUs also want to induce wrong decision at the FC; thus, they can alter both spectrum reports and reputation indexes to this end. Note that MSUs do not care about the resource assignment made by FC.

B. FC Fusion Rule and System dynamics

Since each SU assigns a reputation index to every other SU, due to different assessments a SU can have a wide range to value assigned to it. For example, MSUs can assign 0 to a given SU, while other HSUs give it 1. The FC needs to fuse all reputation indexes reported by the SUs to get a unique reputation value for each SU, as a single number between 0 and 1 describing how reliable that node is. One way to compute it could simply be a mathematical average of all reputation indexes a SU receives. However, such a fusion rule would be rather easy to bias by an MSU, which is an unwanted effect on our goals. Instead, we consider a weighted aggregation rule, to obtain a quantity that we call the global reputation index (GRI) of an SU. The GRI gives a global measure of how much reliable a SU is generally believed to be throughout the network, also taking into account all the reputation indexes of the nodes providing this information. We define the GRI G_i for SU i as:

$$G_i = \frac{\sum\limits_{\ell=1}^{K} g_{\ell,i} \sum\limits_{t=1}^{K} g_{t,\ell}}{\sum\limits_{h\neq i} \sum\limits_{\ell=1}^{K} g_{\ell,h}} \tag{3}$$

In other words, (3) gives G_i as the weighted sum of the reputation indexes of SU i, weighted on the plain arithmetic average of all reputation indexes of the node reporting that index. For example, the weight for the term $g_{j,i}$ is $\frac{1}{K-1}\sum\limits_{\ell=1}^{K} g_{\ell,j}$. Notice that, when weighing over all SUs to get the average, term $\frac{1}{K-1}$ cancels out in (3), since it appears at both numerator and denominator. By definition $g_{i,i} = 0$, so column i is excluded from the sum in the denominator, and is not taken into account in the numerator either.

Now we describe how the FC uses GRIs to assess channel occupancy and assign resource shares to SUs. For each SU i in each location, FC receives the channel sensing reports together with the reputation indexes $\mathbf{g}_i$. We define the sensing report of user i on channel h as c_i^h. In particular, we have that:

$$c_i^h = \begin{cases} 1 \text{ if the channel is sensed busy} \\ 0 \text{ if the channel is sensed idle} \end{cases}$$

for each user $i \in \{1, 2, \ldots, K\}$ and for each channel $h \in \{1, 2, \ldots, N\}$. Hence, we can define the binary vector of all sensing results for user i as $\mathbf{c}_i = [c_i^1, c_i^2, \ldots, c_i^N]$. With the GRIs and the vectors $\mathbf{c}_i$ of each SU i in the location, the FC can infer about channels' occupancy. To do so, it computes the weighted average of spectrum information, using the GRIs as weights. In this way, sensing reports provided by SUs that have a higher probability of being malicious (i.e., a lower GRI) with respect to the others have a reduced impact on the final decision. We define the function

$$\Phi(h) = \frac{\sum\limits_{\ell=1}^{K} c_{h,\ell} G_\ell}{\sum\limits_{\ell=1}^{K} G_\ell}, \quad h = 1, 2, \ldots, N \tag{4}$$

For each channel h, FC computes $\Phi(h)$ and compares the results with a predetermined threshold τ. If $\Phi(h) \leq \tau$ the channel is marked as free, otherwise it is labeled as busy. Moreover, the FC calculates the percentage of resources assigned to each SU. This assignment is also linked to the GRI of a user for two reasons. First of all, although HSUs cooperate during sensing, we aim to discourage selfish behavior by HSU. Moreover, malicious MSUs should get low reputation indexes from HSUs, and thus a lower amount of resources is assigned to them. We hence consider the following formula to compute the percentage of resources R_i assigned to user i:

$$R_i = \frac{G_i}{\sum\limits_{\ell} G_\ell} \tag{5}$$

We now describe the dynamics of the system. The sensing cycle is divided into 5 different stages:

1) FC Request: FC broadcasts a request for spectrum information to the location of interest.
2) Spectrum Sensing: For each of the N channels and by using energy detection technique, the SUs in the location sense the spectrum and decide whether the PU is transmitting.
3) Reporting and Listening: sequentially, each SU reports spectrum occupancy and reputation indexes about neighbors to the FC. In this stage, when it is not transmitting, a SU listens to its neighbors that broadcast their data.
4) Reputation Updating: After all SUs transmitted their data, each SU updates its indexes by comparing the SU's information about spectrum and data broadcast by SUs.
5) Final Decision: FC makes its final decision about channel occupancy and calculates the percentage of resources assigned to every SU. SUs receive from the FC the list of channels and time that they are allowed to use for transmitting data.

While steps 1, 2 and 5 do not depend on the SUs type, during steps 3 and 4 the actions performed by each SUs strongly depend on their type. For example, HSUs and MSUs may report different channel statuses even if they sensed the same channel condition. In particular, the updating rule is described by the following formula:

$$g_{i,j}^{t+1} = \max\{\min\{g_{i,j}^t + \alpha - \beta\chi_i(c_i^t, c_j^t) - \gamma\psi_i(g_i^t, g_j^t), 1\}, 0\} \tag{6}$$

In (6) three quantities are taken into account during the updating process of the index for user j from user i. The first one is the past reputation indexes, $g_{i,j}$, the second one is the function χ_i, which depends on the distance between the two spectrum data vector c_i and c_j, the third one is a function ψ_i that depends on the two vectors of reputation indexes $\mathbf{g}_i$ and $\mathbf{g}_j$. Functions ξ_i and ψ_i depend on i since different users follow a different update rule depending on their type.

In particular, for MSUs, we set the following update rule:

$$g_{i,j}^t = \begin{cases} 0 \text{ if SU } j \text{ is not malicious} \\ 1 \text{ otherwise} \end{cases}, \qquad c_i^t = \neg c_{\text{true}}^t \ \forall t \tag{7}$$

where $\neg c_{\text{true}}^t$ is the opposite of what sensed, as considered in [4]. We also assume that MSUs are performing a coordinated attack, so they are fully aware of the type of the other nodes.

Given this falsification strategy, in the next section we first analyze the requirements that an HSU strategy must have to discourage selfish behavior among HSUs, and then we propose a strategy that makes the system resilient to the presence of noise and MSUs. Indeed, in a real scenario, the sensing results of each SUs may be different, as a consequence of sensing errors. To model noise, we consider two probabilities, P_d and P_f, that are the probability of detecting the PU when it is transmitting and the probability of false alarm, i.e. the probability of detection when PU is not transmitting [14]. We consider that errors during sensing are independent and identically distributed (iid) among devices and we assume that the PU may be transmitting with probability $P_{tx} = 0.5$. These two last statements are justified by the fact that devices are divided into locations based on their physical positions and hence experience the same error probabilities [14] and that we have no information about PU activity.

IV. Game theoretic analysis

A. Perfect Sensing Nash Equilibrium

The first question we address is how the HSUs should behave to guarantee that no one has a positive incentive to adopt a selfish behavior. We start with the perfect sensing case and the presence of HSUs only. We use a game theoretic approach to demonstrate that a HSU has no unilateral incentive to alter its reputation indexes in order to obtain more resources, which implies that HSU reports contain fair sensing and reputation data. We consider the process as a dynamic multistage game [15]. At each stage the players, i.e., the SUs, choose their actions as the reputation and spectrum reports, based on the information they got in the previous stage and the sensed spectrum condition. We model HSU payoff as the percentage of resources they got, as described in 5. We use the concept of Nash equilibrium to demonstrate that, under some assumptions on HSUs, behaving in a selfish way to gain more resources is not rational [15]. Since our game may last for an infinite time, we rely on the overtaking criteria [16] to compare different strategies. To sum up, our game is made by

- Players: K HSUs
- Payoff Function: according to (5)
- Complete Information: all users knows how the reputation index are fused, that is, they know (3) and (5), and they know the reputation indexes other SUs assigned to them at the end of the previous stage
- Infinite game: the game is repeated infinitely many times and players do not discount the future payoffs; this information is also common knowledge among the players.
- Finally, players have the same reaction to belief updates received by others. In particular, we assume that if a HSU i in the previous stage of the game gave indexes $\delta_{i,1}, \delta_{i,2}, \dots, \delta_{i,k}$, then the other HSUs react giving it a reputation index of $\min_{j=1,\dots,k} \delta_{i,j}$ in the current stage.

Notice that our last assumption follows from the rationality of HSUs. Indeed, if an SU i gives an index $g_{i,j} = \delta < 1$ to user j, the GRI of user j decrease. Hence, SU j will react by giving a reputation of $g_{j,i} = \delta$ to SU i. Other HSUs will do the same since a lower reputation index for user j means a lower weight of its assessments and thus a lower GRI for them. Moreover, assigning user i a lower reputation index gives them a higher GRI, without any immediate punishment (even though, due to their rationality, they are able to anticipate future punishments). From now on, we refer to R_i^t as one stage reward or payoff for SUs i, $R_i^{t,2} = R_i^t + R_i^{t+1}$ as the two stage reward for user i, $R^{t,n}$ as the n-stage reward and so on. The following three lemmas are useful to state our main result. For the sake of brevity, their proof is just sketched since a detailed version would be just tedious and technical.

Lemma 1 (Two stage deviation)**.** *If $K > 3$, there is no $\delta < 1$ s.t. $R_i^{t,2} > \frac{2}{K}$ if $\mathbf{g}_i^t = \mathbf{g}_i^{t+1} = \boldsymbol{\delta}_i$ and $\mathbf{g}_j^t = \mathbf{1}_j, \mathbf{g}_j^{t+1} = \boldsymbol{\delta}_j$ for all $j \neq i$, where $\boldsymbol{\delta}_i$ is an all-δ vector (except for the ith element, that is irrelevant anyways), and $\mathbf{1}_j$ is an all-1 vector.*

This lemma shows that the reward cannot be improved by a two stage deviation in which one player changes its reputation of the other players to gain a better reward. The proof implies to show, first, that one such deviation should be identically applied by player i to all other players $j \neq i$, since this dominates deviations where only some $j \neq i$, but not all of them, are affected. Second, it is also possible to show that even a deviation where all other players' reputation is identically decreased cannot beneficial; this happens because in the second stage of the deviation, these players will retaliate on the deviating player with the same deviation, and player i can anticipate this kind of behavior. A rigorous proof can be just obtained through enumeration of all possible alternatives following this sketch. Using this lemma, one can demonstrate another one as a corollary.

Lemma 2 (Multi stage deviation)**.** *There is no sequence of $\boldsymbol{\delta}^t, \boldsymbol{\delta}^{t+1} \dots, \boldsymbol{\delta}^{t+n} \neq 1, 1, \dots, 1$ s.t. $\mathbf{g}_i^t = \boldsymbol{\delta}^t, \mathbf{g}_i^{t+1} = \boldsymbol{\delta}^{t+1}, \dots, \mathbf{g}_i^{t+n} = \boldsymbol{\delta}^{t+n}$, $R_i^{t,n} > \frac{n+1}{K}$.*

This is just a generalization of Lemma 1, which can be shown similarly. It is worth noting that this kind of extension is analogous to what has been proven for multistage games about the deviation principle [15], which is actually a consequence of the Bellman-Ford optimality applied to the extensive form of the dynamic game seen as a tree. Simply put, any supposed improvement over a subgame should necessarily include a shortcut that is also an improvement, because the overall reward is just the sum of the partial rewards. Thus, if a strategy is not improvable over a given number of stages, it cannot be improved over a higher number of stages either. The last lemma we need is the following.

Lemma 3 (Infinite stage deviation)**.** *For any sequence* $\mathbf{g}_i^t > \mathbf{g}_i^{t+1} > \mathbf{g}_i^{t+2} \dots$ $\exists T$ *s.t.* $R_i^{t+\ell} < \frac{1}{K}$ $\forall \ell \geq T$.

This lemma is less trivial instead, as it implies a deviation also on infinitely many stages. However, it is just sufficient to prove that any deviation (also including infinite ones) with decreasing reputations becomes disadvantageous after a certain stage T, with finite T, onwards. All of these results combined with the overtaking critierion can lead to the following theorem, which is the key theoretical result of our contribution in this paper.

Theorem 1. *Suppose we have:*

- *Perfect channel correlation among neighbors, that is,* $P_d = 1, P_f = 0$
- *No MSU in the system*
- *At least 4 SUs, i.e.,* $K \geq 4$
- *Rational behavior of HSUs, as defined before*

Then reporting reputation 1 *among HSUs is a Nash Equilibrium.*

Proof. Since HSUs play the game indefinitely many times, they decide their strategy caring about not only the resources they get in the present stage but also those that FC will assign to them in the next rounds. Thus, in order to prove the theorem, we show that any unilateral deviation from the strategy $g_{i,j} = 1$ does not lead to any advantage. To compare rewards for infinite strategy, we adopt the overtaking criterion [16], defined as follows. Consider two strategies, $\{\boldsymbol{\delta}\} = \boldsymbol{\delta}^1, \boldsymbol{\delta}^2, \dots$ and $\{\boldsymbol{\delta}'\} = \boldsymbol{\delta}'^1, \boldsymbol{\delta}'^2, \dots$. We will say that strategy $\{\boldsymbol{\delta}\}$ is preferred to $\{\boldsymbol{\delta}'\}$ if

$$0 < \liminf_{T\to\infty} \sum_{t=1}^{T} (R^t(\boldsymbol{\delta}'^t) - R^t(\boldsymbol{\delta}^t)) \qquad (8)$$

where $R^t(\boldsymbol{\delta}^t)$ is the reward at time t when playing strategy $\boldsymbol{\delta}$ for a generic user For the sake of a simpler notation, we omit the user subscript and we will also omit R^t in the further usage of the above formula (8) when comparing strategy with overtaking criterion, so we will just write "$\boldsymbol{\delta}'^t - \boldsymbol{\delta}^t$" inside the limit or whenever comparing strategies. Now, consider the strategy $\{\mathbf{e}\} = \mathbf{e}^1, \mathbf{e}^2, \dots$ where $\mathbf{e}^t = \mathbf{1}$ $\forall t$. It is straightforward to see that $R^t(\mathbf{e}) = \frac{1}{K}$ for every t and every HSU. Moreover, consider any other strategy $\{\boldsymbol{\delta}\} = \boldsymbol{\delta}^1, \boldsymbol{\delta}^2, \dots$ s.t. $\exists t : \boldsymbol{\delta}^t \neq \mathbf{e}^t$. Thus, at some point δ deviates from the strategy $\{\mathbf{e}\}$. We have three cases:

- $\boldsymbol{\delta}$ is a deviation that stays forever at a value δ^* less then one; that is, if $\boldsymbol{\Delta}^*$ is a reputation report where a user assigns value δ^* to others, $\boldsymbol{\delta} = \dots, \mathbf{1}, \mathbf{1}, \boldsymbol{\Delta}^*, \boldsymbol{\Delta}^*, \dots,$ and then we have
$$\liminf_{T\to\infty} \sum_{t=1}^{T} (\mathbf{e}_t - \boldsymbol{\delta}_t) = +\infty \qquad (9)$$
since after the first step, we the difference is always greater than 0, due to what found in Lemma 1.
- $\boldsymbol{\delta}$ deviates from $\mathbf{e}$ only for a finite number of steps. Then there must be a set of indexes $t_1, t_2, \dots, t_h$ s.t. the reputations played are $\delta_{t_1} < 1, \delta_{t_2} < 1, \dots, \delta_{t_h} < 1$ and afterwards $\delta_{t_h+1} = 1$. As proven in Lemma 2, in this case $R^{t,(h+1)}(\boldsymbol{\delta}) - R^{t,h}(\boldsymbol{\delta})$ is less than $\frac{h+1}{K}$, thus
$$\liminf_{T\to\infty} \sum_{t=1}^{T} (\mathbf{e}_t - \boldsymbol{\delta}_t) > 0 \qquad (10)$$
- $\boldsymbol{\delta}$ has an infinite deviation of the type $1 > \delta_{t_1} > \delta_{t_2} \dots$. We demonstrate that there is no sequence of δ_t that can lead to a reward greater that $\frac{1}{K}$ for an arbitrarily long time, so we have:
$$\liminf_{T\to\infty} \sum_{t=1}^{T} (\mathbf{e}_t - \boldsymbol{\delta}_t) = +\infty \qquad (11)$$
since there exists L s.t. $R^t(\boldsymbol{\delta})$ is less than $\frac{1}{K}$, $\forall t > L$.

Notice that due to Lemmas 1, 2 and 3, any other type of strategy is dominated by one of the three described before. Thus, we demonstrated that no unilateral deviation, finite or infinite, leads to an advantage for a given HSU when the overtaking criterion is used. This proves that $\mathbf{e}$ is a Nash equilibrium [15]. □

We also remark that the proof shown above does not imply that other Nash equilibria may exist. However, it is also possible to show along the same lines that stronger results hold. Also this part is omitted for the sake of simplicity. However, the Nash equilibrium identified above can be shown to be sequentially rational and therefore subgame perfect. This is to say, because feedback report $\mathbf{e}$ is not only a Nash equilibrium but is non-improvable over multiple stage deviations, it is the only possible rational outcome.

B. MSU impact and HSU noise resilient strategy strategy

After identifying a strategy for HSUs that leads to a desirable equilibrium in case of no MSUs and perfect sensing conditions, we now analyze how the impact of MSUs and noise during sensing can affect the system. The first question to address is how to choose the threshold τ for the channel occupancy.

1) Channel occupancy threshold: Consider the case where ℓ users out of K report wrong information due to either sensing errors or malicious behavior. If the channel is busy, i.e., the PU is transmitting, according to equation 4 we have that the FC makes the correct decision if and only if:

$$\frac{(K-\ell)\cdot 1+0\cdot\ell}{k}\geq\tau \tag{12}$$

A similar equation can be formulated for the case of idle channel:

$$\frac{(k-\ell)\cdot 0+1\cdot\ell}{k}<\tau \tag{13}$$

By combining (12) and (13), we see that the optimal threshold is $\tau = 0.5$. By selecting this threshold in case of perfect sensing, our system can tolerate up to $\lceil\frac{K}{2}\rceil - 1$ MSUs in the system. Notice that this is the maximum amount of malicious users that any distributed system that does not rely on a central/privileged unit can tolerate.

2) Probability distribution of the Hamming distance between two reports: We now introduce the possibility of errors in the channel sensing process. Given the detection probability P_d, the false alarm probability P_f and the primary user transmission probability P_tx the sensing error probability on one channel can be expressed as:

$$P_e = (1-P_d)P_{tx} + (1-P_{tx})P_f. \tag{14}$$

that is, P_e is the probability that a device misdetect the state of one of the N channels. Consider now two devices i and j and their spectrum reports on one channel, denoted as S_i and S_j, respectively. The probability that there is a mismatch on channel sensing is given by:

$$P_m = P(S_i = 1, S_j = 0) + P(S_i = 0, S_j = 1) \tag{15}$$

That can be rewritten as:

$$P_m = 2(1-P_{tx})(1-P_f)P_f + 2P_{tx}(1-P_d)P_d \tag{16}$$

Now consider the case of N channels and suppose that the probability of mismatch among the two reports is iid for each of them. We have that each channel error can be modeled as a Bernoulli distributed random variable, with probability of success P_m. Thus we have that the Hamming distance between two reports, which is denoted as$mis_{i,j} = ||S_i - S_j||$, is a random variable with binomial distribution with parameters P_m and N.

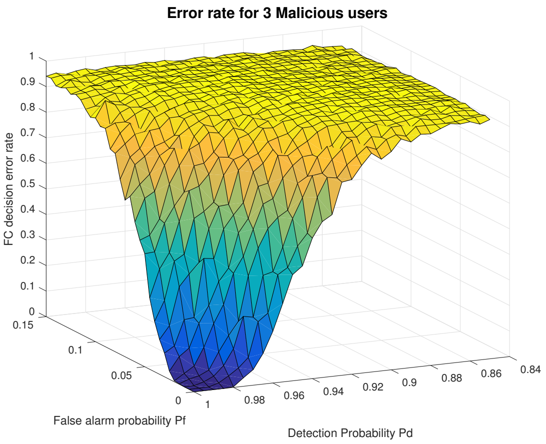


Fig. 2: FC error rate when HSUs uses a strategy that does not consider noise

3) Noise resilient HSU strategy: Although HSUs do not intentionally lie on spectrum reports, there can be differences among their reports due to sensing errors. If a naïve strategy that does not take into account sensing errors is used by HSU, the reputations among users easily decrease and reach 0. This happens because as soon there is an error in sensing, the reputation is lowered down. In this scenario, MSUs can easily strongly influence the FC decision, as shown in Fig. 2Thus, there is the need to design a strategy resilient to sensing errors. We seek a strategy that allows SUs to tolerate sensing mistakes up to a certain amount if their behavior follows the rationality condition of (1). Hence, we propose an improved update rule as a novel contribution, described in the following equation.

$$g_{i,j}^{t} = \begin{cases} \min\{\alpha + g_{i,j}^{t-1}, 1\} \text{ if } g_j^{t-1} = g_j^{*t-1}, |\mathbf{c}_i - \mathbf{c}_j| < \xi \\ \max\{g_{i,j}^{t-1} - \max\limits_h (g_{i,h} - g_{j,h}) - \frac{|C_i - C_j|}{N}, 0\} \text{ if not} \end{cases} \tag{17}$$

where here $\mathbf{g}^*$ are the reputation indexes that user j should give according to the common updating rule. Essentially, if a user is coherently seen to update its reputation reports according to a collaborative updating rule, other users also slightly increase its reputation. This happens only if this user does not make any mistake in its sensing report, though. If this happens because the user is an MSU, it is correct not to increase its reputation. If instead this happens because of sensing errors, it will compensate in the long run, unless the user is an HSU that is particularly bad or unlucky at sensing the channel, but in this case it shows no macroscopic difference with a malicious user. The increase in reputation is a tunable parameter α that in the following evaluations is set to 0.1. The choice of α implies a trade off between the need for fast recovery of the reputation among devices and the protection against MSUs behavior. Another parameter is ξ which is the number of channels over which we allow the sensing report to disagree. The choice of ξ is based on a statistical analysis of the error distribution. On one hand, a possible choice would be to set $\xi = N + 1$, implying that the sensing reports are not considered and only the mutual reputation matters. This leads to a simple majority rule to determine the reputation, which we will take as a benchmark for our evaluations. On the other hand, ξ should not be set to an extremely low value, since this leads to a fast decreasing reputation in the presence of disagreements on the channel state, which would, in turn, destroy collaboration and trust among HSUs. Thus, in order to select the most appropriate value for ξ, we analyze the distribution of the rv $mis_{i,j}$. We would like to choose a value for ξ s.t. $\Pr(mis_{i,j} > \xi) \approx 0$ to support the correct reporting from the HSUs, but we want to distinguish between

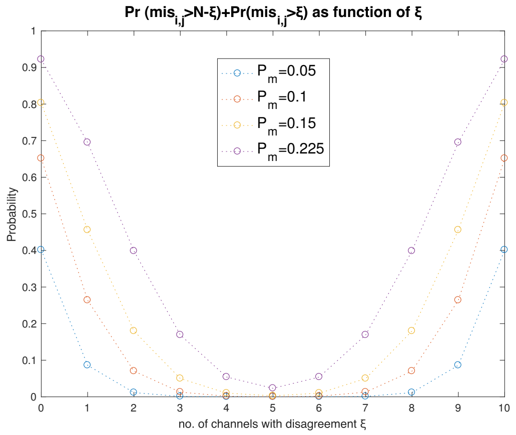


Fig. 3: Distribution of the sum of the two probabilities

HSU and MSU reports by setting a sufficiently high ξ. Under the assumption that MSU simply reports a false (logical-not) sensing result on every one of the N channels, the distance between their report and the ground truth would be equal to N minus the numbers of their sensing mismatches, that happen to be correct instead. Since we want to minimize the probability that a MU goes undetected, we can write the condition as $\Pr(mis_{i,j} > N - \xi) \approx 0$. Hence, we will select ξ as the solution of the following problem:

$$\xi = \underset{x=1,2,\dots,N}{\arg\min} \left(\Pr(mis_{i,j} > N - x) + \Pr(mis_{i,j} > x)\right) \quad (18)$$

Fig. 3 depicts the value of $\Pr(mis_{i,j} > N-x) + \Pr(mis_{i,j} > x)$ for $x = 1, 2, \dots, 10$ and for various values of P_m. It is possible to see how in our specific system $\xi = 5$ is the minimum of the function for all values of P_m and hence it is the best choice when $N = 10$, as set during our simulation.

V. Numerical Results

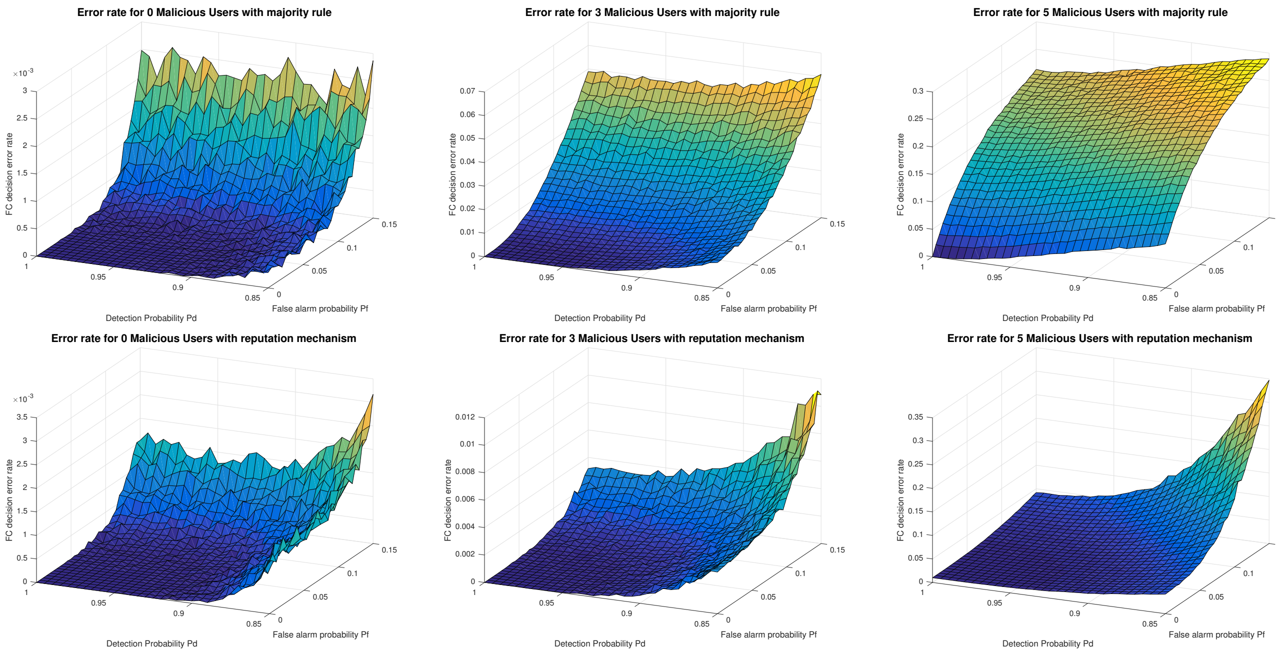
In this section, we present the results obtained from the numerical simulation of the system. We consider $N = 10$ channels, $K = 12$ users and we let P_d and P_m vary from 1 to 0.85 and from 0 to 0.15, respectively. The transmission probability P_{tx} is 0.5 and the threshold ξ is empirically set to 5. HSUs adopt the updating strategy described in (17), while MSUs adopt the strategy described in (7). In this setting, we focus on the FC error rate and how it depends on the amount of MSUs in the system. We vary the number of MSUs from 0 to 5. For each setting, we run 100 Monte Carlo trials, each of 100 sensing rounds. As a benchmark, we also run simulations in the same amount where the FC implements a simple majority rule.

In panel a of figure 4 the performances of the two systems without MSUs are reported. Although the system has good performances also with majority rule, the performances decrease dramatically as soon as sensing error probability increases. However, while a simple majority report is very prone to this error amplification, our proposed fusion mechanism is based on avoiding this phenomenon and keep making correct decisions most of the time even when sensing errors are within acceptable limits. When 3 MSUs are introduced in the system, which is shown in panel b of fig. 4, the overall performance becomes worse for both our proposal and the benchmark of the majority-based fusion rule. However, the degradation in our proposed mechanism is graceful as the exploitation of correlated channel sensing and the forgiving update rule in the reputation of truthfully reporting users allow the system to robustly handle the presence of some malicious users. This is still true when 5 MSUs, which is a considerable share of the total number of $K = 12$, are introduced. The results are shown in panel c of fig 4. Indeed, the larger is the number of MSUs in the system, the larger is the gap between our mechanism and the majority rule. In this case, even with a considerably high presence of MSUs, our mechanism exhibits an error rate in the fusion decision that is always more than 5 times lower than the benchmark. Further, the shapes of the two curves are substantially different. While the one obtained by a majority rule fusion mechanism increases constantly with P_m, our mechanism exhibits a low error rate that increases slowly when the values of P_m are low but rises up very fast after P_m exceed a certain amount. Notice also that the concavity of the majority rule curve changes, which implies that even a moderate false alarm or undetected PU probabilities cause the fusion rule to be inaccurate. On the other hand, our proposed fusion strategy remains accurate, and the FC error rate explodes only when sensing errors are frequent. Thus, even though the performance of our proposed mechanism is naturally affected by system noise, it is shown to perform efficiently and considerably mitigate the impact of MSUs.

VI. Conclusions and Future Work

We proposed a reputation-based mechanism to perform efficient distributed channel sensing in a CRN that employs such a paradigm to detect PU transmission, while at the same time mitigating the impact of malicious users. First, we gave a thorough analysis of the rationality of truthful reporting via game theory; indeed, our system exploits the channel correlation among devices and the concept of reputation to reduce the effects of malicious users giving false reports. By using a game theoretic approach, we demonstrated that the introduction of reputation reports incentivizes honest users to cooperate at the sensing process without introducing new security threats. We also analyzed the effect of noise and malicious users presence on the system and provide details on how to design a noise resilient strategy able to reduce the damage from malicious users.

Finally, we numerically showed the effectiveness of the proposed solution via simulation. Combining truthful reporting from the HSUs with the appropriate strategy for data fusion can considerably reduce the FC error rate with respect to a simple majority fusion rule. We showed that our mechanism is effective even when malicious users and sensing errors are simultaneously found in the system. However, our simulations also show that the channel sensing correlation assumption cannot be arbitrarily relaxed. This is coherent with our design



(a) 0 MSU

(b) 3 MSUs

(c) 5 MSUs

Fig. 4: FC decision error rate with 0,3 and 5 MSUs. In top line the majority rule was used, the bottom implemented our reputation mechanism.

rationale: we created the mechanism so that spatial correlation can be used to oust malicious users from the network and hence a certain amount of correlation must be present to let the mechanism work properly. Future works should focus on the optimal strategy for MSU in order to find which equilibrium can be reached and how it depends on malicious users percentage and noise level. In this spirit, a possible extension of the present contribution would be to introduce dynamically tunable reporting and fusion mechanisms so as to adapt them to a variable number of malicious users and/or time-varying channel conditions that induce variable sensing error rates. This can lead to a more sophisticated dynamic policy that can also be studied through game theory. Another extension would be to consider other malicious behaviors rather than just falsely reporting the opposite of reality, e.g., based on random reporting and/or MSUs that are only intentionally lying over a small fraction of reports. This can be done via Bayesian game theory and paves the way for interesting extensions based on automated reasoning to identify and counteract more complex network attacks, to guarantee improved security.

References

[1] C. W. Paper, "Cisco visual networking index: Global mobile data traffic forecast update, 2016-2021," Tech. Rep., March 2017.

[2] M. Khasawneh and A. Agarwal, "A survey on security in cognitive radio networks," in *2014 6th International Conference on Computer Science and Information Technology (CSIT)*, March 2014, pp. 64–70.

[3] A. Khattab, D. Perkins, and M. Bayoumi, *Cognitive Radio Networks: From Theory to Practice*. Springer, 01 2013.

[4] O. León and K. P. Subbalakshmi, *Cognitive Radio Network Security*. Singapore: Springer Singapore, 2017, pp. 1–30.

[5] J. M. Peha, "Approaches to spectrum sharing," *IEEE Communications Magazine*, vol. 43, no. 2, pp. 10–12, Feb 2005.

[6] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.*, vol. 1, Nov 2004, pp. 772–776 Vol.1.

[7] Z. Qin, Y. Gao, and M. D. Plumbley, "Malicious user detection based on low-rank matrix completion in wideband spectrum sensing," *IEEE Transactions on Signal Processing*, vol. 66, no. 1, pp. 5–17, Jan 2018.

[8] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 13, no. 2, pp. 86–95, Sep. 2009.

[9] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, Feb 2011.

[10] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "Arc: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1707–1719, Aug 2014.

[11] M. Najimi, A. Ebrahimzadeh, S. M. H. Andargoli, and A. Fallahi, "Energy-efficient sensor selection for cooperative spectrum sensing in the lack or partial information," *IEEE Sensors Journal*, vol. 15, no. 7, pp. 3807–3818, July 2015.

[12] M. Ghaznavi and A. Jamshidi, "A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network," *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1810–1816, March 2015.

[13] L. Ma, Y. Xiang, Q. Pei, Y. Xiang, and H. Zhu, "Robust reputation-based cooperative spectrum sensing via imperfect common control channel," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3950–3963, May 2018.

[14] F. F. Digham, M. S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Transactions on Communications*, vol. 55, no. 1, pp. 21–24, Jan 2007.

[15] S. Tadelis, *Game Theory an Introduction*. Princeton University Press, 2013.

[16] A. Rubinstein, "Equilibrium in supergames with the overtaking criterion," *Journal of Economic Theory*, vol. 21, no. 1, pp. 1 – 9, 1979.