Secure Cooperative Spectrum Sensing and Access Against Intelligent Malicious Behaviors

Wei Wang*, Lin Chen†, Kang G. Shin‡ and Lingjie Duan§
*Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China
†Laboratoire de Recherche en Informatique (LRI), University of Paris-Sud 11, Orsay 91405, France
‡Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109-2121, U.S.A.
§Engineering Systems and Design Pillar, Singapore University of Technology and Design, Singapore

***Abstract*—Sensing falsification is a key security problem in cooperative spectrum sensing for cognitive radio networks. Most previous approaches assume that malicious users only cheat in their sensing reports following a predefined rule. However, some malicious users usually act intelligently to strategically adjust their malicious behavior according to their objectives and the network's defense schemes. The existing schemes cannot resist the malicious behaviors of intelligent malicious users (IMUs) without long-term collection of information on their reputation. In this paper, we construct a moral hazard principal-agent framework and design an incentive compatible mechanism to thwart the malicious behaviors of rational and irrational IMUs. We find that neither spectrum sensing nor spectrum access alone can prevent the malicious behavior without any information on users' reputation. According to the analysis of malicious behavior resistance methods, we propose a joint spectrum sensing and access mechanism to optimally prevent the IMUs from sensing falsification. Our evaluation results show that the proposed mechanism achieves almost the same performance as the ideal case with perfect sensing.**

I. Introduction

Over the past few years, cooperative spectrum sensing [1] has been shown to offer significant performance gains to incumbent detection in cognitive radio (CR) networks [2]. Multiple spectrum sensors report their measurements of primary signal strength to a fusion center, which makes a final decision on the presence/absence of any licensed primary user nearby.

In cases where the measurements are collected from multiple sensors without any prior trust in them, which is commonly the case for many CR applications, even a small number of malicious users can exploit cooperative spectrum sensing to significantly degrade the system performance or even cripple the system. In [3], malicious attacks are categorized as incumbent emulation and sensing data falsification. Recently, authentication schemes have been proposed to effectively thwart incumbent emulation [4], [5]. To further prevent sensing data falsification of malicious users, we focus on the design of *malicious-behavior-resistance* (MBR) mechanisms. Most existing approaches assume that malicious behaviors are predefined and the malicious users can be identified. By contrast, we account for more practical aspects, which, in turn, introduces new technical challenges as follows.

The ultimate goal of malicious users is to obtain their own "utilities", rather than just causing erroneous sensing decisions. It is thus important to investigate *intelligent malicious users* (IMUs) who adjust their behaviors adaptively to the system's MBR mechanisms to maximize their own utilities. Obviously, the presence of these IMUs makes the MBR design and configuration more challenging.

The reputation-based approach detects malicious users based on their report statistics. However, it needs sophisticated authentication for the identification of malicious users, and takes a long time to observe their behavior and establish reliable reputation metrics. Therefore, the reputation-based approach is unsuitable for usually fast-changing CR networks like those used for vehicular systems. Without any *a priori* established reputation metric, MBR is likely to incur a high *resistance cost*, i.e., falsely classifying some honest users as malicious and thus degrading the network performance.

Motivated by the above two technical challenges (i.e., the presence of IMUs and the absence of their reputation information), we propose a principal-agent-based joint spectrum sensing and access framework to thwart the malicious behaviors of IMUs in CR networks. This paper makes the following main contributions.

- **Moral Hazard Principal-Agent Framework**: We construct a principal-agent framework [6] that offers IMUs incentives not to report falsified sensing results. Since the IMUs cannot be identified directly, it is necessary to consider the risk of moral hazard [7] and design the punishment based on their sensing outcome. We use exclusion of IMUs from spectrum sensing and access as a punishment for their malicious behavior. Specifically, we model MBR with the moral hazard principal-agent framework to design a spectrum sensing and access mechanism with both the participation and the incentive compatibility constraints.
- **Malicious Behavior Analysis**: We consider both rational and irrational IMUs. The malicious behaviors are analyzed according to the utilities of different types of IMUs. The penalty factor of primary–secondary

The work of W. Wang is supported by National Natural Science Foundation of China (Nos. 61261130585, 61001098), and Natural Science and Technology Specific Major Projects (No. 2012ZX03002009). The work of L. Chen is supported by the ANR (Agence Nationale de la Recherche) under the grant Green-Dyspan (ANR-12-IS03).

978-1-4799-3360-0/14/$31.00 © 2014 IEEE

users' collision is exploited as the conditions for IMUs to choose different malicious behaviors. The malicious behavior analysis provides an important basis to design appropriate MBR mechanisms.

- **Joint Spectrum Sensing and Access Mechanism**: Without any information on users' reputation, both spectrum sensing and spectrum access are required to provide an effective incentive to thwart the malicious behavior. By analyzing the resistance cost of MBR methods, we derive the conclusion that the MBR via spectrum sensing could provide an infinite punishment with resistance cost, while the MBR via spectrum access provides a limited punishment without any resistance cost. Based on the analysis, we propose optimal joint spectrum sensing and access mechanisms that provide an appropriately large incentive to IMUs with the least resistance cost.

The rest of this paper is organized as follows. Section II introduces our system model and problem formulation while Section III models this problem as a principal-agent framework. Section IV analyzes the behaviors of rational and irrational IMUs. Sections V studies the optimal MBR mechanisms against both types of IMUs. Section VI numerically evaluates the proposed MBR mechanisms. The related work is reviewed in Section VII and the paper concludes with Section VIII.

II. Cooperative Spectrum Sensing Model in the Presence of Malicious Users

We consider a generic model of CR networks consisting of a set $\mathscr{N} = \{1, \cdots, N\}$ of secondary users (SUs) who opportunistically exploit the spectrum of primary users (PUs). PUs are encouraged to share unused spectrum with SUs and would be compensated if the collision occurs between PU and SU. Each SU is equipped with a sensor to discover spectrum holes. The SUs' sensing results are reported to a controller (e.g., base station or access point) which uses the SUs' sensing reports to make a final decision on the presence/absence of PUs and then allocates the available spectrum to the SUs. This process is a sort of cooperative spectrum sensing that can increase sensing accuracy by eliminating sensing errors due to hidden terminals and signal fading for certain SUs.

Mathematically, the spectrum sensing at an individual SU is characterized by the following hypothesis test:

$$Y = \begin{cases} X + \sigma^2 & \mathcal{H}_1, \\ \sigma^2 & \mathcal{H}_0, \end{cases} \tag{1}$$

where X is the strength of the primary signal sensed by an SU in the presence of a PU, σ^2 is the power of the thermal noise, $\mathcal{H}_0$ and $\mathcal{H}_1$ are the hypotheses that the spectrum status is "0" ("1") indicating the absence (presence) of any primary activity.

The performance of each SU's spectrum sensor is characterized by the probability of misdetection, denoted as P_m, and the probability of false alarm, denoted as P_f. Formally, P_m and P_f can be expressed as:

$$P_m = \Pr\{\mathcal{S}_0^{(i)}|\mathcal{H}_1\},\ P_f = \Pr\{\mathcal{S}_1^{(i)}|\mathcal{H}_0\},\ \forall i \in \mathscr{N} \tag{2}$$

where $\mathcal{S}_0^{(i)}$ and $\mathcal{S}_1^{(i)}$ denote the individual sensing result of SU i to be 0 and 1, respectively.

Let $\mathcal{R}_0^{(i)}$ and $\mathcal{R}_1^{(i)}$ denote SU i reporting 0 and 1, respectively. The honest user reports his sensing result to the controller, $\Pr(\mathcal{R}_0^{(i)}|\mathcal{S}_0^{(i)}) = \Pr(\mathcal{R}_1^{(i)}|\mathcal{S}_1^{(i)}) = 1$, while the IMU deliberately reports a false sensing result according to his malicious behavior 'script'. A malicious behavior is determined to maximize the IMU's utility. We assume that the number of IMUs is much smaller than that of honest users; otherwise, no solution will work.

The controller's decision is characterized by two hypotheses, denoted as $\hat{\mathcal{H}}_1$ and $\hat{\mathcal{H}}_0$, indicating that the decision of cooperative spectrum sensing is 1 and 0, respectively. In this paper, we adopt the "OR" sensing rule, the simplest and most widely applied cooperative sensing rule characterized by its stringent protection on the primary activities [8]. However, our approach can be easily extended to other rules. Fig. 1 illustrates the relationship among the spectrum status, the sensing results, the sensing reports and the controller's decision.

Unlike most existing approaches to cooperative sensing, here we focus on the design of a joint MBR mechanism for final sensing decision and actual allocation of the sensed spectrum to each SU if the decision is $\hat{\mathcal{H}}_0$. Specifically, the joint MBR mechanism is denoted as $\boldsymbol{\rho} \triangleq (\rho_S, \rho_A)$, where ρ_S and ρ_A are the spectrum-sensing and the spectrum-access policies, respectively.

In case of collision between PUs and SUs, the PU system would be compensated and a penalty would thus be imposed on the SU system. Let α be the penalty factor of primary–secondary users' collision, capturing the tradeoff between the system throughput and the impact on the primary network. If all SUs follow the controller's spectrum-access policy and a collision occurs, all of them are responsible and share the ensuing penalty; otherwise, the penalty is imposed on the particular SU who violates the controller's allocation policy.

The controller acts on behalf of all SUs and needs to choose an appropriate joint spectrum sensing and access policy $\boldsymbol{\rho}$ so as to maximize the aggregate expected utility of all honest SUs in sharing the licensed spectrum. Here, we normalize the total spectrum benefit to be 1. The problem can then be formulated as

$$\max_{\boldsymbol{\rho}}\ U(\boldsymbol{\rho}) = (1 - \theta(\boldsymbol{\rho}))(\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) - \alpha \Pr(\mathcal{H}_1\hat{\mathcal{H}}_0)) \tag{3}$$

where $\theta(\boldsymbol{\rho})$ is the ratio of the spectrum allocated to the IMUs to the total sensed spectrum holes under the policy $\boldsymbol{\rho}$, $\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)$ is the probability that the controller successfully identifies a spectrum hole, $\Pr(\mathcal{H}_1\hat{\mathcal{H}}_0)$ is the probability that the controller falsely decides on the absence of primary activity, although a PU is active. Note that the probability of the controller's decision $\hat{\mathcal{H}}_0$ depends on the spectrum-sensing policy ρ_S.

III. Principal-Agent-Based Malicious Behavior Resistance by Spectrum Sensing and Access

We now model cooperative spectrum sensing as a moral hazard principal-agent framework [6][7], where the "*principal*" is the controller that makes the final sensing decision and then allocates the available spectrum to the SUs, and the "*agents*" are the SUs to sense the spectrum. The "*moral hazard*" arises

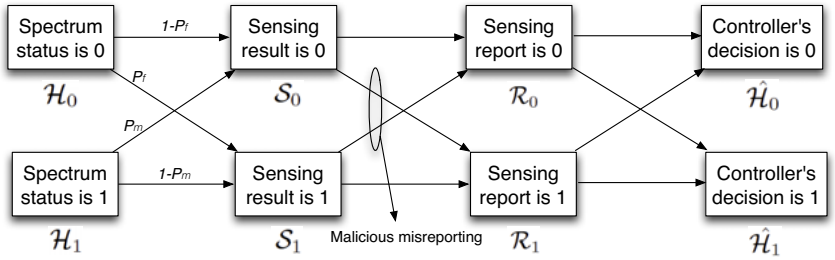


Fig. 1. Cooperative spectrum-sensing model with malicious behavior

in the framework, since the SUs may have an incentive to misreport the sensing results if the interests of the agent and the principal are not aligned. The controller does not know whether a user reports the information different from his true sensing result, and can only observe the final reported results, i.e., the actions of the users are hidden from the controller. This is consistent with the relationship between the principal and the agent in economics. Based on the principal-agent framework, we would like to design MBR mechanisms to thwart the malicious behavior of IMUs. We first present a model and then study some important structural properties. In the analysis that follows, for simplicity, we consider the case of a single IMU to describe the principal-agent framework and derive MBR mechanisms against different types of malicious behavior. With a known number of IMUs, the analysis could be also applicable to a group of cooperative IMUs.

A. The Principal-Agent Model

The principal-agent model [6][7] motivates the agent to act on behalf of the principal. The procedure of a classic principal-agent model includes:

1) The principal provides the contract to the agents;
2) The agents decide to accept or reject the contract;
3) The agents select one of multiple actions available;
4) The principal makes a payment decision for agents based on their outcome.

We must consider the following key components of cooperative spectrum sensing in the presence of IMUs.

- *Agents' actions*: The IMUs will report their sensing results correctly or incorrectly, which correspond to the high- and low-effort actions, respectively, in the principal-agent model, denoted by A_h (honest report) and A_m (malicious report). Obviously, the controller would like to incentivize the users to choose A_h.
- *Cost of agents*: Actions A_h and A_m will respectively incur costs C_h and C_m to the agents. For the honest action A_h, the corresponding $C_h = 0$. With the malicious action A_m, the IMU could achieve the benefit of sensing falsification. To make it consistent with the principal-agent model, we consider the falsification benefit as a negative cost of IMU of choosing A_m, and thus $C_m < 0$.
- *Utility of agents*: If the controller acquires a spectrum hole successfully, it will allocate the hole to the user, which is considered as a payment/reward. The user i's utility u_i is the sum of the received payment from the controller and its cost.
- *The principal's return*: By collecting the sensing results from SUs, the controller makes a final decision on the presence/absence of PUs. If an available spectrum opportunity is discovered, the utilized spectrum resource is the return of the principal. On the other hand, if the controller makes a wrong decision and generates collision with PUs, its return would be negative, a punishment by the primary system.
- *Utility of the principal*: The system utility U is the sum of the utilities of all honest users, as expressed in Eq. (3). It can also be calculated by the return minus the spectrum resource allocated to the IMUs.

Remark 1 (Moral Hazard): There exists "moral hazard" since the actions of IMUs are hidden from the controller. In this case, the IMUs may misreport the sensing results if the interests of the agent and the principal are not aligned. Therefore, it is necessary to design MBR mechanisms based on the sensing outcome to thwart malicious behaviors, i.e., avoiding the risk of moral hazard.

B. How to Thwart Malicious Behaviors?

In the principal-agent model, an MBR strategy should satisfy the following two essential constraints.

- *Participation constraint*: The principal provides a non-negative expected utility to the agents, i.e., $u_i(A_h) \geq 0, \forall i$.
- *Incentive compatibility constraint*: The agent achieves a higher expected utility when it obeys the principal's policy than that when it violates, i.e., $u_i(A_h) \geq u_i(A_m), \forall i$.

Here we establish two basic structural properties of the principal-agent model in cooperative sensing in the presence of IMUs and provide some insights in how to thwart them.

Considering the participation constraints of all honest users, we can obtain the following lemmas.

Lemma 1: A necessary condition for the secondary system with N users to access the spectrum is that the penalty factor α for the primary–secondary collision should satisfy

$$\alpha \leq \frac{\Pr(\mathcal{H}_0)}{\Pr(\mathcal{H}_1)} \left(\frac{1 - P_f}{P_m} \right)^N . \tag{4}$$

Proof: The participation constraint should be met to guarantee the honest users to participate in sharing spectrum with PUs, i.e., let $u_i \geq 0$ for all honest users i. The system utility $U \geq 0$ if the utilities of all honest users are positive. In other words, $U \geq 0$ is a necessary condition of $u_i \geq 0$ for all honest users i.

$$U = \Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) - \alpha \Pr(\mathcal{H}_1\hat{\mathcal{H}}_0). \quad (5)$$

Let's consider the best case when all N users are honest, then the system utility is

$$U = \Pr(\mathcal{H}_0)(1-P_f)^N - \alpha \Pr(\mathcal{H}_1)P_m^N \geq 0. \quad (6)$$

Since the above equation shows the utility of the best case, the equation is a necessary condition of $U \geq 0$. Therefore, the lemma holds. ■

Lemma 2: To protect the primary system, the lower bound of the punishment factor α should be

$$\alpha > \Pr(\mathcal{H}_0)/\Pr(\mathcal{H}_1). \quad (7)$$

Proof: To prevent the SUs' unbridled access, the primary system always adjusts the punishment factor to prevent the IMU who transmits data without spectrum sensing. The participation constraint of this type of users need not be satisfied, i.e.,

$$u = \Pr(\mathcal{H}_0) - \alpha \Pr(\mathcal{H}_1) < 0, \quad (8)$$

so the lemma holds. ■

Remark 2 (Feasible Region of α): The above two lemmas provide upper and lower bounds for the punishment factor α from the PU system's perspective. The PUs are encouraged to share their spectrum with SUs, but might not allow the SUs to access the spectrum without sensing. These bounds provide a feasible region of α, which is an important basis for the SU system to design the MBR mechanisms.

Since the controller regards those users who reported minority results as suspicious, it has the following two mechanisms to cope with IMUs and provide the incentives, which will be investigated in the analysis that follows.

- *MBR via Spectrum Sensing* ρ_S (MBR-S): The controller excludes the sensing results reported by suspicious users with probability ω_S.
- *MBR via Spectrum Access* ρ_A (MBR-A): The controller does not allocate the spectrum access opportunity to suspicious users with probability ω_A. Other users with the access right share the spectrum equally.

Note that ω_S and ω_A are the aggregate exclusion probabilities over multiple time slots, so they could be larger than 1, e.g., $\omega_S = 2$ indicates that the sensing results of the suspicious users would be excluded in the following two time slots.

Remark 3 (Agent/Resistence Cost): To thwart the malicious behaviors, the controller using MBR would possibly classify some honest users as malicious falsely and exclude them from cooperative sensing because of the existence of moral hazard. Thus, the controller suffers the agent/resistance cost, i.e., degrading the network performance.

In the proposed MBR mechanism, besides using spectrum access to adjust the payments, we use spectrum sensing to adjust the cost of a malicious agent, which is different from the classic principal-agent model, in which the cost does not change with the principal's mechanism.

IV. Malicious Behavior Analysis

There are various attack strategies that the IMUs can launch, depending on their objectives. So, these attack strategies, captured by the corresponding models, may differ in effectiveness, and may also call for different defense strategies. We categorize the IMUs into the following two types according to their motivation.

1) *Rational IMU*: A rational IMU aims to maximize its own utility, which is obtained by the accessible spectrum minus the penalty imposed on it;
2) *Irrational IMU*: An irrational IMU aims to cause the most damage possible to the system, i.e., minimizing the system utility defined in Eq. (3).

The rational IMU is the most common type of malicious users who maximize their utility from a selfish perspective. On the contrary, the objective of irrational IMUs is not to maximize their utility but cause as large negative effect on the system utility as possible, which is the worst case. Both are assumed to have the information of the underlying MBR mechanism and adjust their behaviors intelligently.

A. Rational IMU

A rational IMU aims to maximize his spectrum resource, which can be achieved in two ways. First, the rational IMU utilizes the allocated channel resource when the controller's decision is $\hat{\mathcal{H}}_0$. Second, the rational IMU alone occupies the channel when the controller's decision is $\hat{\mathcal{H}}_1$.

The following lemma analyzes the case of aggressive channel occupation of the rational IMU.

Lemma 3: If the controller's decision is $\hat{\mathcal{H}}_1$, the rational IMU should not transmit except for the case when he purposely falsifies the sensing result from $\mathcal{S}_0$ to $\mathcal{R}_1$.

Proof: The utility of the rational IMU can be calculated as

$$u = \Pr(\mathcal{H}_0|\hat{\mathcal{H}}_1) - \alpha \Pr(\mathcal{H}_1|\hat{\mathcal{H}}_1). \quad (9)$$

For the case when 0 is reported as a sensing result but the controller's final decision is $\hat{\mathcal{H}}_1$, at least one honest user gets the sensing result 1. The utility can be calculated as

$$u = \frac{\Pr(\mathcal{H}_0)(1-(1-P_f)^{N-1}) - \alpha \Pr(\mathcal{H}_1)(1-P_m^{N-1})}{\Pr(\mathcal{H}_0)(1-(1-P_f)^{N-1}) + \Pr(\mathcal{H}_1)(1-P_m^{N-1})}. \quad (10)$$

Substituting Eq. (7) in Lemma 2 into the utility, P_f and P_m become usually less than 0.5, and obviously, $u < 0$.

For the case when both the sensing and reporting results are 1, we can obtain his expected utility as

$$u = \frac{\Pr(\mathcal{H}_0)P_f - \alpha \Pr(\mathcal{H}_1)(1-P_m)}{\Pr(\mathcal{H}_0)P_f + \Pr(\mathcal{H}_1)(1-P_m)}. \quad (11)$$

Similarly, substituting Eq. (7) in Lemma 2 into the above expression, the utility is negative. ■

The utilities achieved by the rational IMU with different sensing and reporting results are listed in Table I, where $\theta(\rho_A)$ is the spectrum allocated to the IMU by the controller according to the policy ρ_A.

TABLE I. RATIONAL IMU UTILITIES

sensing	reporting	$\mathcal{H}_0\hat{\mathcal{H}}_0$	$\mathcal{H}_0\hat{\mathcal{H}}_1$	$\mathcal{H}_1\hat{\mathcal{H}}_0$	$\mathcal{H}_1\hat{\mathcal{H}}_1$
$\mathcal{S}_0$	$\mathcal{R}_0$	$\theta(\rho_A)$	0	$-\alpha/N$	0
$\mathcal{S}_0$	$\mathcal{R}_1$	$\theta(\rho_A)$	1	$-\alpha/N$	$-\alpha$
$\mathcal{S}_1$	$\mathcal{R}_0$	$\theta(\rho_A)$	0	$-\alpha/N$	0
$\mathcal{S}_1$	$\mathcal{R}_1$	$\theta(\rho_A)$	0	$-\alpha/N$	0

B. Irrational IMU

The objective of an irrational IMU is to reduce the system utility, which is the aggregate accessible spectrum of other honest users. The spectrum allocated to the irrational IMU can be considered as its utility, which is decreasing w.r.t. the spectrum of honest users. When the controller's decision is $\hat{\mathcal{H}}_1$ but the PU is absent, the wasted channel opportunity can also be considered as the irrational IMU's utility. Besides the above two cases similar to the rational IMU, the irrational IMU can also increase the punishment to the system caused by primary–secondary collision by cheating from $\mathcal{S}_1$ to $\mathcal{R}_0$. The irrational IMU does not utilize the channel to transmit data so that the punishment of a single user can be avoided for the irrational IMU. The utilities achieved by an irrational IMU in different scenarios are listed in Table II.

TABLE II. IRRATIONAL IMU UTILITIES

sensing	reporting	$\mathcal{H}_0\hat{\mathcal{H}}_0$	$\mathcal{H}_0\hat{\mathcal{H}}_1$	$\mathcal{H}_1\hat{\mathcal{H}}_0$	$\mathcal{H}_1\hat{\mathcal{H}}_1$
$\mathcal{S}_0$	$\mathcal{R}_0$	$\theta(\rho_A)$	1	$\alpha-\alpha/N$	0
$\mathcal{S}_0$	$\mathcal{R}_1$	$\theta(\rho_A)$	1	$\alpha-\alpha/N$	0
$\mathcal{S}_1$	$\mathcal{R}_0$	$\theta(\rho_A)$	1	$\alpha-\alpha/N$	0
$\mathcal{S}_1$	$\mathcal{R}_1$	$\theta(\rho_A)$	1	$\alpha-\alpha/N$	0

In the next section, we explore the MBR mechanisms for thwarting rational and irrational IMUs, respectively, according to their different objectives and corresponding malicious behaviors.

V. OPTIMAL JOINT SPECTRUM SENSING AND ACCESS FOR MALICIOUS BEHAVIOR RESISTANCE

We now design the optimal joint spectrum sensing and access mechanisms for MBR against rational and irrational IMUs. Our basic idea is to satisfy the incentive compatibility constraint to incentivize the SUs to report the sensing results honestly.

MBR mechanisms can be designed in three steps. First, we investigate malicious behavior without MBR which will be used as a reference for comparison. Second, neither MBR-S nor MBR-A alone can prevent malicious behaviors. Third, MBR-S and MBR-A are adopted jointly and their parameters are optimized according to the analysis of resistance costs.

By the optimal joint spectrum sensing and access of MBR mechanisms, the IMU is motivated to report honestly with the least resistance cost, so the CR system can thwart the IMU successfully and achieve the maximal system utility. The user index i is omitted for simplicity of presentation.

A. Thwarting Rational IMU

Based on Lemma 3, it is possible for the rational IMU to achieve a larger utility by misreporting $\mathcal{R}_1$ when the sensing result is $\mathcal{S}_0$. The probability of spectrum status when the actual sensing result is $\mathcal{S}_0$, can be calculated as

$$\Pr(\mathcal{H}_0|\mathcal{S}_0) = \frac{\Pr(\mathcal{H}_0)(1-P_f)}{\Pr(\mathcal{H}_0)(1-P_f)+\Pr(\mathcal{H}_1)P_m} \tag{12}$$

$$\Pr(\mathcal{H}_1|\mathcal{S}_0) = \frac{\Pr(\mathcal{H}_1)P_m}{\Pr(\mathcal{H}_0)(1-P_f)+\Pr(\mathcal{H}_1)P_m}. \tag{13}$$

We investigate the case without MBR to analyze the necessary condition of MBR.

Lemma 4: Without any MBR mechanism, if the punishment factor α satisfies

$$\alpha < \frac{\Pr(\mathcal{H}_0)(1-P_f)(1-(1-P_f)^{N-1}/N)}{\Pr(\mathcal{H}_1)P_m(1-P_m^{N-1}/N)}, \tag{14}$$

the rational IMU always reports 1 when the sensing result is 0.

Proof: If the rational IMU reports honestly with the sensing result of 0, the expected utility is

$$u(A_h) = \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-1}/N - \Pr(\mathcal{H}_1|\mathcal{S}_0)P_m^{N-1}\alpha/N. \tag{15}$$

If the rational IMU misreports from $\mathcal{S}_0$ to $\mathcal{R}_1$, without MBR, the final sensing decision is 1. The expected utility of a rational IMU to transmit data is

$$u(A_m) = \Pr(\mathcal{H}_0|\mathcal{S}_0) - \Pr(\mathcal{H}_1|\mathcal{S}_0)\alpha. \tag{16}$$

The rational IMU would misreport the sensing result when the expected utility of misreporting is larger than that of honest reporting. Using the above two equations, we derive the condition of α. ■

If α satisfies Eq. (14), we need to design an MBR mechanism to prevent the malicious behavior. Let $u(A, \boldsymbol{\rho})$ denote the rational IMU's utility achieved with the MBR mechanism $\boldsymbol{\rho}$. The goal of MBR mechanism $\boldsymbol{\rho}$ is to make the expected utility of reporting true sensing results larger than that of reporting false results, i.e., $u(A_h, \boldsymbol{\rho}) \geq u(A_m, \boldsymbol{\rho})$. We first consider the two types of MBR mechanism separately.

By adopting MBR-S, the controller excludes the reported result with probability ω_S. It is possible for the controller to misclassify some honest users as suspicious ones, affecting the number of effective users in cooperative spectrum sensing. The expected number of excluded users is estimated to be:

$$N_S = \left(\Pr(\mathcal{H}_0)P_f + \Pr(\mathcal{H}_1)P_m\right)N\omega_S. \tag{17}$$

Let $\omega_S(t)$ be the exclusion probability in MBR-S at time slot t. The following lemma deals with the allocation of exclusion probability over time for a given aggregate exclusion probability.

Lemma 5: Given an aggregate exclusion probability ω_S, different exclusion probability distributions $\omega_S(t)$ achieve the same total utility for the rational IMU.

Proof: If the rational IMU cheats from 0 to 1, with the exclusion probability $\omega_S(t)$, the expected utility of a rational IMU in the current slot is

$$\begin{aligned} u(A_m,(\omega_S,0)) &= \Pr(\mathcal{H}_0|\mathcal{S}_0)\left(\omega_S(t)(1-P_f)^{N-N_S-1}1/N \right. \\ &\quad \left. +(1-\omega_S(t)(1-P_f)^{N-N_S-1})\right) \\ &\quad -\Pr(\mathcal{H}_1|\mathcal{S}_0)\left(\omega_S(t)P_m^{N-N_S-1}\alpha/N \right. \\ &\quad \left. +(1-\omega_S(t)P_m^{N-N_S-1})\alpha\right). \end{aligned} \quad (18)$$

From the above equation, we find the utility function to be linear in the exclusion probability within the slot. Thus, given an aggregate exclusion probability, the exclusion probability distribution over time does not affect the performance of MBR. ■

The following lemma shows that MBR-S only is ineffective in thwarting malicious behavior.

Lemma 6: MBR-S alone cannot prevent the rational IMU's malicious behavior.

Proof: With MBR-S only, the utility of rational IMU for reporting honestly is

$$\begin{aligned} u(A_h,(\omega_S,0)) &= \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-N_S-1}/N \\ &\quad -\Pr(\mathcal{H}_1|\mathcal{S}_0)P_m^{N-N_S-1}\alpha/N. \end{aligned} \quad (19)$$

Comparing Eqs. (18) and (19), it is always satisfied that

$$u(A_h,(\omega_S,0)) \geq u(A_m,(\omega_S,0)). \quad (20)$$

Both sides of this inequation are equal only if $\omega_S(t)=1$.

In this case, a suspicious user would be excluded forever from the cooperative spectrum sensing, $\omega_S \to +\infty$. However, this is not practical since it would also exclude honest users due to their sensing errors. ■

Obviously, the rational IMU's utility decreases as the aggregate exclusion probability ω_S increases because its reported result is ignored. With a large enough ω_S, the malicious behavior can be prevented. However, the MBR-S mechanism also reduces the system utility because some results reported from honest users are ignored, which is considered as the resistance cost.

Lemma 7: The upper bound of ω_S in the MBR-S mechanism is

$$\omega_S < \frac{N-1-\log_{\frac{1-P_f}{P_m}}\frac{\alpha\Pr(\mathcal{H}_1)}{\Pr(\mathcal{H}_0)}}{(\Pr(\mathcal{H}_0)P_f+\Pr(\mathcal{H}_1)P_m)\,N}. \quad (21)$$

Proof: With MBR-S, the system utility is:

$$\begin{aligned} U &= \frac{N-1}{N}\left(\Pr(\mathcal{H}_0)(1-P_f)^{N-N_S-1} \right. \\ &\quad \left. -\alpha\Pr(\mathcal{H}_1)P_m^{N-N_S-1}\right). \end{aligned} \quad (22)$$

The upper bound of ω_S should be satisfied to ensure that the system utility is positive. Therefore, Eq. (21) follows. ■

Using MBR-A only, the controller reduces the probability of allocating the spectrum resource to the suspicious user.

Lemma 8: MBR-A alone cannot prevent the rational IMU's malicious behavior.

Proof: If the aggregate exclusion probability ω_A in MBR-A is large enough, the sensed spectrum holes would not be allocated to IMUs. Without MBR-S, the rational IMU can occupy all the spectrum holes for transmission by reporting "1" irrespective of the sensing results, so the system has no chance to allocate the spectrum. With MBR-A only, the rational IMU's utilities for honest and malicious reports are

$$\begin{aligned} u(A_h,(0,\omega_A)) &= \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-1}/N \\ &\quad -\Pr(\mathcal{H}_1|\mathcal{S}_0)P_m^{N-1}\alpha/N \end{aligned} \quad (23)$$

$$u(A_m,(0,\omega_A)) = \Pr(\mathcal{H}_0|\mathcal{S}_0)-\Pr(\mathcal{H}_1|\mathcal{S}_0)\alpha. \quad (24)$$

The condition of rational IMU's malicious reporting is

$$u(A_h,(0,\omega_A)) < u(A_m,(0,\omega_A)), \quad (25)$$

which can be rewritten as

$$\alpha < \frac{\Pr(\mathcal{H}_0)}{\Pr(\mathcal{H}_1)}\frac{(1-P_f)-(1-P_f)^N/N}{P_m-P_m^N/N}. \quad (26)$$

It is always satisfied by Lemma 4. ■

Based on Lemmas 6 and 8, neither MBR-S nor MBR-A alone can prevent the rational IMU's malicious behavior. Therefore, it is necessary to adopt both MBR-S and MBR-A to design a joint spectrum sensing and access mechanism.

Although the aggregate exclusion probability ω_A of MBR-A could be large, it should be considered only for a few slots because the rational IMU can continue to misreport the sensing result and transmit data, possibly achieving more utility than the punishment. The probability of the rational IMU's malicious behavior can be calculated as

$$\begin{aligned} \Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1) &= (\Pr(\mathcal{H}_0)(1-P_f)+\Pr(\mathcal{H}_1)P_m) \\ &\quad \cdot(1-\omega_S(t)(1-P_f)^{N-N_S-1}). \end{aligned} \quad (27)$$

According to Lemma 5, different exclusion probability distributions $\omega_S(t)$ would not change the punishment. Without loss of generality, we set the same exclusion probability $\omega_S(t)$ for each time slot. Given the aggregate exclusion probability ω_S for one-time malicious behavior, $\omega_S(t)$ can be calculated as

$$\omega_S(t) = \omega_S \Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1). \quad (28)$$

Substituting Eq. (27) into this equation, $\omega_S(t)$ is obtained as

$$\begin{aligned} &\omega_S(t) = (\omega_S(\Pr(\mathcal{H}_0)(1-P_f)+\Pr(\mathcal{H}_1)P_m)) \quad (29) \\ &/\left(1+\omega_S(\Pr(\mathcal{H}_0)(1-P_f)+\Pr(\mathcal{H}_1)P_m)(1-P_f)^{N-N_S-1}\right) \end{aligned}$$

Adopting MBR-A can reduce the rational IMU's utility when the spectrum hole is discovered.

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) = \Pr(\mathcal{H}_0)\omega_S(t)(1-P_f)^{N-N_S-1}. \quad (30)$$

Although MBR-A also excludes some honest users from spectrum access, all the honest users have the same exclusion probability, so no resistance cost is caused by MBR-A.

Remark 4 (Properties of MBR-S and MBR-A): Based on the above analysis, we conclude that the punishment by MBR-S could be infinite, while that by MBR-A is upper-bounded. However, MBR-A applies the punishment without any resistance cost.

So, we propose a MBR mechanism for thwarting the rational IMU next.

Optimal MBR Mechanism for Rational IMU:

Because MBR-A incurs no resistance cost but its punishment is upper-bounded, the aggregate exclusion probability of MBR-A is set to be large enough:

$$\omega_A = \left\lceil \frac{\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)}{\Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1)} \right\rceil \tag{31}$$

where $\lceil\cdot\rceil$ is the ceiling operation.

According to the principal-agent model, the optimal MBR scheme is to adjust the punishment level so that the expected utilities for honest and malicious reports are the same. The optimal solution is to find ω_S within the feasible region of Lemma 4 via a one-dimensional search such that

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)/N = \Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1)\Delta u(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1) \tag{32}$$

where $\Delta u(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1)$ is the rational IMU's expected utility for misreporting once. Here, $\Delta u(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1) = 1$.

B. Thwarting Irrational IMU

The irrational IMU's utility conflicts with the system utility. It is difficult to provide the irrational IMU an effective incentive based on the classic principal-agent model. Fortunately, in our problem, the cost C_m for malicious reports depends on the MBR mechanism, which is different from the classical principal-agent model. This difference makes it possible to design a MBR mechanism to prevent the irrational IMU's malicious behavior.

Based on the analysis in Section V, the irrational IMU can cheat from $\mathcal{S}_0$ to $\mathcal{R}_1$ and from $\mathcal{S}_1$ to $\mathcal{R}_0$. The basic idea of the optimal MBR mechanism for an irrational IMU is similar to that for a rational IMU, but there exist some differences because of the different objectives between rational and irrational IMUs.

Lemma 9: Without any MBR mechanism, the irrational IMU always reports 1 when the sensing result is 0. It reports 0 when the sensing result is 1 if the penalty factor α satisfies

$$\alpha > \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-1}P_f}{\Pr(\mathcal{H}_1)P_m^{N-1}(1-P_m)}. \tag{33}$$

Proof: Without MBR, the irrational IMU's utility for honest reporting when the sensing result is 0, is

$$u(A_h) = \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-1}\frac{1}{N} \tag{34}$$

the utility for cheating from 0 to 1 is

$$u(A_m) = \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-1} - Pr(\mathcal{H}_1|S_0)P_m^{N-1}\alpha\frac{N-1}{N}. \tag{35}$$

The irrational IMU misreports when

$$\alpha > \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N}}{\Pr(\mathcal{H}_1)P_m^{N}} \tag{36}$$

which conflicts with Lemma 1, so the irrational IMU's report will always cheat from 0 to 1 in the absence of MBR.

The difference between the irrational IMU's utilities for honest reporting and cheating when the sensing result is 1 is

$$-\frac{N-1}{N}\Pr(\mathcal{H}_0|S_1)(1-P_f)^{N-1} + \Pr(\mathcal{H}_1|S_0)P_m^{N-1}\alpha\frac{N-1}{N}. \tag{37}$$

Thus, the condition of cheating is

$$\alpha > \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-1}P_f}{\Pr(\mathcal{H}_1)P_m^{N-1}(1-P_m)}. \tag{38}$$

■

By using similar methods as those for rational IMU, we can obtain the following three lemmas. Due to space limitation, we omit their proofs.

Lemma 10: Given an aggregate exclusion probability ω_S, different exclusion probability distributions $\omega_S(t)$ achieve the same total utility for the irrational IMU.

Lemma 11: MBR-S alone cannot prevent the irrational IMU's malicious behavior.

Lemma 12: MBR-A alone cannot prevent the irrational IMU's malicious behavior.

To achieve a low resistance cost of MBR, we justify whether or not the two types of misreporting exist by the punishment factor α according to Lemma 9, and then design the optimal MBR mechanisms.

Optimal MBR Mechanism for Irrational IMU:

1) If $\frac{\Pr(\mathcal{H}_0)}{\Pr(\mathcal{H}_1)} < \alpha < \frac{\mathcal{H}_0(1-P_f)^{N-1}P_f}{\mathcal{H}_1P_m^{N-1}(1-P_m)}$, then the irrational IMU would report $\mathcal{R}_1$ when the sensing result is $\mathcal{S}_0$. The probability of the irrational IMU's malicious behavior is

$$\Pr(\mathcal{S}_0\mathcal{R}_1) = \Pr(\mathcal{H}_0)(1-P_f) + \Pr(\mathcal{H}_1)P_m. \tag{39}$$

The exclusion probability for each time slot is

$$\omega_S(t) = \omega_S(\Pr(\mathcal{H}_0)(1-P_f) + \Pr(\mathcal{H}_1)P_m). \tag{40}$$

The probability of discovering the spectrum holes is

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) = \Pr(\mathcal{H}_0)\omega_S(t)(1-P_f)^{N-N_S-1}. \tag{41}$$

To resist the malicious behavior, MBR-A is adopted without any resistance cost. The aggregate exclusion probability ω_A is set as

$$\omega_A = \left\lceil \frac{\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)}{\Pr(\mathcal{S}_0\mathcal{R}_1)} \right\rceil. \tag{42}$$

We derive the optimal ω_S by satisfying:

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)/N = \Pr(\mathcal{S}_0\mathcal{R}_1)u(\mathcal{S}_0\mathcal{R}_1) \tag{43}$$

where

$$u(\mathcal{S}_0\mathcal{R}_1) = \frac{N-1}{N}(1-\omega_S(t))\left(\Pr(\mathcal{H}_0)(1-P_f)^{N-N_S} - \alpha\Pr(\mathcal{H}_1)P_m^{N-N_S}\right) \tag{44}$$

2) If $\frac{\mathcal{H}_0(1-P_f)^{N-1}P_f}{\mathcal{H}_1 P_m^{N-1}(1-P_m)} < \alpha < \frac{Pr(\mathcal{H}_0)(1-P_f)^{N-1}}{\Pr(\mathcal{H}_1)P_m^{N-1}}$, then we must consider both types of misreporting. The probability of discovering the spectrum holes is

$$\begin{aligned}\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) &= \Pr(\mathcal{H}_0)\omega_S(1-P_f)^{N-N_S-1} \\ &\quad + \Pr(\mathcal{H}_0)P_f(1-\omega_S(t))(1-P_f)^{N-N_S-1}.\end{aligned} \tag{45}$$

Since $\Pr(\mathcal{S}_0\mathcal{R}_1) + \Pr(\mathcal{S}_1\mathcal{R}_0) = 1$, $\omega_S(t)$ is equal to ω_S. ω_A is set as

$$\omega_A = \lceil \Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) \rceil. \tag{46}$$

Obviously, $\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) < 1$, so ω_A is set to 1 in this case.

Similarly, ω_S can be optimized to satisfy

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)/N = \Delta u \tag{47}$$

where Δu is the average increased irrational IMU's utility due to misreporting, which is calculated as in Eq. (48):

$$\begin{aligned}\Delta u &= \left(\Pr(\mathcal{H}_0)(1-P_f)^{N-N_S} - \alpha\Pr(\mathcal{H}_1)P_m^{N-N_S}\right) \\ &\quad \cdot (1-\omega_S(t))\frac{N-1}{N} \\ &\quad + \left(\alpha\Pr(\mathcal{H}_1)(1-P_m)P_m^{N-N_S-1}\right. \\ &\quad \left. - \Pr(\mathcal{H}_0)P_f(1-P_f)^{N-N_S-1}\right)\frac{N-1}{N}.\end{aligned} \tag{48}$$

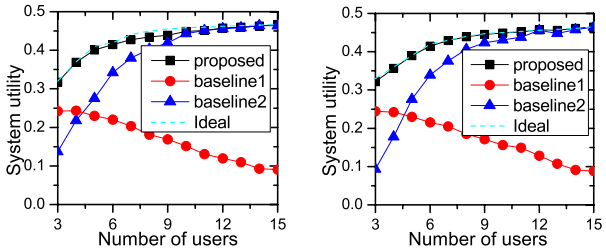
VI. Evaluation

We now evaluate the performance of the proposed MBR mechanisms using simulation. In the simulation, there are 5 users ($N = 5$) one of whom is malicious. The controller can adjust the sensing error probabilities P_f and P_m to maximize the system utility subject to $P_f + P_m = 0.1$. As to the spectrum status, we set $\Pr(\mathcal{H}_0) = \Pr(\mathcal{H}_1) = 0.5$. The penalty factor of primary–secondary users' collision is set to 5.

First, we show the performance of the proposed MBR mechanism in Fig. 2 while varying the number of users. We consider three baseline schemes for performance comparison.

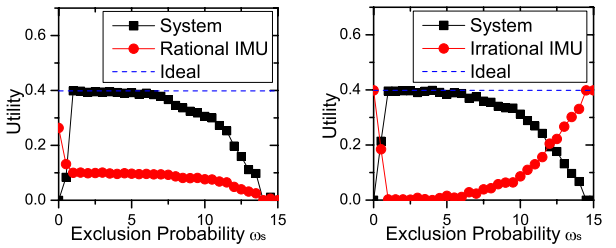
- Ideal sensing: The controller can detect all false reports of sensing results and equally share the spectrum among all users.
- Baseline 1 (Carrot-and-Stick) [13]: The users stop cooperation when the malicious behavior is discovered, and restore cooperation after a certain period.
- Baseline 2 (Fixed punishment) [14]: The fixed values of ω_S are used to exclude the IMUs from cooperative sensing. The value of ω_S is set to 10 in this simulation.

Our results indicate that the proposed MBR mechanism achieves almost the same performance as the ideal sensing scheme, which could be considered as an upper bound. In [14], the punishment could be set as a large enough fixed value, because the IMUs are detected correctly, such that the punishment does not cause any resistance cost. Considering the resistance cost, a large cost is incurred if ω_S is too large, and the malicious behavior cannot be prevented if ω_S is too small. Therefore, the proposed MBR mechanism outperforms the fixed punishment scheme.

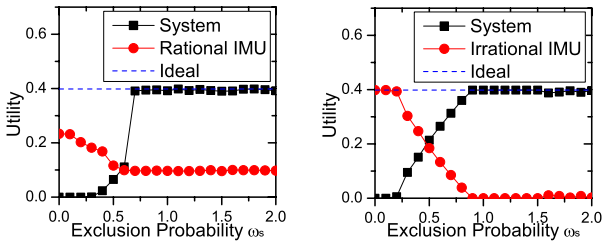


(a) Rational IMU (b) Irrational IMU

Fig. 2. Performance comparison



(a) Rational IMU ($0 \le \omega_S \le 15$) (b) Irrational IMU ($0 \le \omega_S \le 15$)

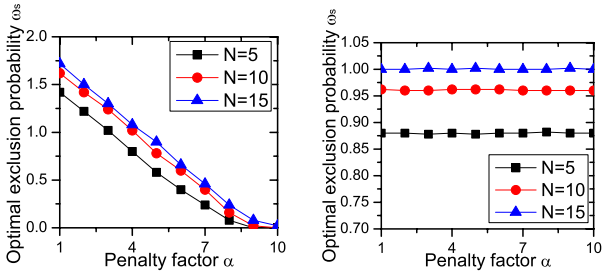


(c) Rational IMU ($0 \le \omega_S \le 2$) (d) Irrational IMU ($0 \le \omega_S \le 2$)

Fig. 3. Effect of the aggregate exclusion probability ω_S

The Carrot-and-Stick scheme does not perform well without accurate reputation metrics, because all users stop cooperation in the presence of malicious behavior. Although it thwarts the malicious behaviors successfully, the normal sensing errors cause frequent termination of cooperation. The proposed MBR mechanism stops the cooperation with IMUs only, not the entire cooperation.

Next, we investigate the key parameter in our proposed mechanism, the aggregate exclusion probability ω_S, to show the necessity of the discussion in Section 5 and analyze the effects of ω_S on the system utility, as plotted in Fig. 3. As ω_S increases, the utility of the IMU decreases, demonstrating that the proposed MBR mechanism can reduce the IMU's utility. There is a jump in the system utility curve, a result of the IMU's stop of dishonest reports. With an increasing ω_S, the system can provide more effective resistance to the malicious behavior, so the system utility increases until the jump point. On the right of the jump point, the system utility decreases because of the resistance cost. Figs. 3(c) and 3(d) show the details around the jump point. It is observed that the jump point for the rational IMU increases the system utility significantly, while the improvement at the jump point for the irrational IMU is not so obvious. This is because the controller has the incentive compatible MBR mechanism with the rational IMU, and has the opposite objective to the irrational IMU. From this analysis, we can find that the jump point occurs at the optimal



(a) Rational IMU (b) Irrational IMU

Fig. 4. Optimal aggregate exclusion probability ω_S

ω_S in the MBR mechanism, where the maximal system utility is achieved.

Fig. 4 shows the optimal ω_S while varying the penalty factor α and the number of users N. As the penalty factor gets larger, the required ω_S for thwarting the malicious behavior is smaller, because a large penalty factor increases the IMU's risk, i.e., punished with a higher probability because of the primary–secondary users' collision. Fig. 4(b) shows that the penalty factor α has little effect on the optimal value of ω_S. The irrational IMU just reports false sensing results but does not transmit using the spectrum holes, thus avoiding the risk of primary–secondary users' collision penalty. In fact, the optimal ω_S would decrease if α is large enough. According to the conditions of the irrational IMU's malicious behavior in Lemma 9, the intersection of the curves and the horizontal axis occurs at a point with a huge α, e.g., $\alpha = 2.5 \times 10^6$ for $N = 5$. In addition, one can find that the optimal ω_S for the rational IMU is larger for a larger number of users.

VII. Related Work

Secure cooperative spectrum sensing has been studied extensively as a key technology for reliable detection of primary users in CR networks. In [9], a robust reputation-based fusion scheme for sensing data is proposed based on the Byzantine failure model. In [10], the reputation-based scheme is investigated with the assistance of some trusted users. As mentioned earlier, it takes a long time to build a reliable reputation. Other researchers focused on the detection of attackers. In [11], a malicious user is detected based on a fading correlation analysis. In [12], the effect of information imbalance between the attackers and the system is analyzed for independent and dependent attacks. These threshold-based attacker detection schemes cannot prevent the malicious behavior if the malicious users are intelligent, for example, adopting an attack-and-run strategy.

Use of an economic theory is effective in cooperative sensing, which does not require to differentiate honest users from malicious ones. In [13], all users stop spectrum sensing if some selfish user deviates from the cooperation "standard". Utilizing a repeated game model, the selfish users are forced to cooperate. In [14], indirect and direct punishment strategies are proposed for attack prevention. The malicious users are detected by the primary–secondary users' collision when the cooperative sensing decision is "busy", which would not misjudge the honest users as malicious and avoid the resistance cost. However, this mechanism is not suitable for some malicious users who do not access the spectrum, e.g., the irrational IMUs. When malicious users cannot be detected deterministically, the punishment by adjusting the cooperative spectrum sensing strategy is ineffective in preventing the malicious behavior because of its resistance cost. Adopting a moral hazard principal-agent model, we consider spectrum access together with spectrum sensing to thwart the malicious behavior of IMUs.

VIII. Conclusion

In this paper, we proposed a moral hazard principal-agent-based joint spectrum sensing and access framework to thwart both rational and irrational IMUs. By analyzing the malicious behavior of both types of IMUs, we explored the properties of the penalty factor of primary–secondary users' collision, which is of importance to the reduction of resistance cost. Since neither spectrum sensing nor spectrum access alone can prevent the malicious behaviors, we have designed optimal joint spectrum sensing and access MBR mechanisms based on the properties of MBR-S and MBR-A. Our numerical results show that the proposed MBR mechanism achieves almost the same performance as the ideal sensing scheme and outperforms other existing schemes.

References

[1] A. Ghasemi, E.S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," *Proc. IEEE DySPAN 2005*, pp. 131–136, Nov. 2005

[2] J. Mitola, G. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999

[3] R. Chen, J.M. Park, Y.T. Hou, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008

[4] S. Anand, Z. Jin, K.P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks", *Proc. of IEEE DySPAN 2008*, pp. 1–6, Oct. 2008

[5] Y. Liu, P. Ning, H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," *Proc.of IEEE Symposium on Security and Privacy*, May 2010

[6] J. Laffont, D. Martimort, "*The theory of incentives I: The principal-agent model*," Princeton University Press, Princeton NJ, U.S., 2001

[7] P. Bolton, M. Dewatripont, "*Contract theory*," MIT Press, Dec. 2004

[8] A. Ghasemi, E. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *J. Commun.*, vol. 2, no. 2, pp. 71–82, Mar. 2007

[9] R. Chen, J.M. Park, K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *Proc. of IEEE INFOCOM 2008*, Apr. 2008

[10] K. Zeng, P. Pawelczak, D. Cabric, "Reputation-based Cooperative Spectrum Sensing with Trusted Nodes Assistance," *IEEE Commun. Letters*, vol. 14, no. 3, pp. 226–228, Mar. 2010

[11] A.W. Min, K.G. Shin, X. Hu, "Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks," *Proc. of IEEE ICNP 2009*, Oct. 2009

[12] H. Li, Z. Han, "Catching Attacker(s) for Collaborative Spectrum Sensing in Cognitive Radio Systems: An Abnormality Detection Approach," *Proc. of IEEE DySPAN 2010*, Apr. 2010

[13] C. Song, Q. Zhang, "Achieving cooperative spectrum sensing in wireless cognitive radio networks," *ACM Mobile Comput. Commun. Rev.*, vol. 13, no. 2, pp. 14–25, Apr. 2009

[14] L. Duan, A. Min, J. Huang, K.G. Shin, "Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1658–1665, Oct. 2012