This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

Thwarting Intelligent Malicious Behaviors in Cooperative Spectrum Sensing

Wei Wang, *Member, IEEE*, Lin Chen, *Member, IEEE*,
Kang G. Shin, *Life Fellow, IEEE*, Lingjie Duan, *Member, IEEE*

Abstract—Sensing falsification is a key security threat in cooperative spectrum sensing in cognitive radio networks. Intelligent malicious users (IMUs) adjust their malicious behaviors according to their objectives and the network's defense schemes. Without long-term collection of information on users' reputation, the existing schemes fail to thwart such malicious behaviors. In this paper, we construct a joint spectrum sensing and access framework to thwart the malicious behaviors of both rational and irrational IMUs. Lack of reputation information makes the malicious behavior resistance degrade performance since the honest users may be misjudged as IMUs. Based on the moral hazard principal-agent model, we design an incentive compatible mechanism to provide a moderate punishment to IMUs. Our findings show that neither spectrum sensing nor spectrum access alone can prevent malicious behaviors without any information on users' reputation. According to the different properties of malicious behavior resistance by spectrum sensing and spectrum access, we employ joint spectrum sensing and access to optimally prevent the IMUs sensing falsification. The proposed malicious behavior resistance mechanism is shown to achieve almost the same performance as the ideal case with truthful sensing.

Index Terms—Wireless security, cognitive radio, cooperative spectrum sensing, principal-agent model

1 Introduction

Over the past few years, cooperative spectrum sensing [2], [3] has been shown to offer significant performance gain in incumbent detection in cognitive radio (CR) networks [4], [5], [6]. Multiple secondary users (SUs) report their measurements of the signal strength from primary users (PUs) to a fusion center, which makes a final decision on the presence/absence of any licensed PU nearby.

In cases where the sensing results are collected from the SUs without any prior information on users reputation, which is the case for many decentralized CR applications, even a small number of malicious users can sabotage cooperative spectrum sensing to significantly degrade the system performance or even paralyze the system. Malicious attacks in CR spectrum sensing can be categorized into two types, *incumbent emulation* and *sensing data falsification* [7]. Recently, several authentication schemes have been proposed to effectively cope with the incumbent emulation attack [8], [9]. We consider the latter type of malicious attacks in this paper.

Specifically, we focus on the design of *malicious behavior resistance* (MBR) mechanisms to thwart the sensing data falsification attack. In contrast to most existing approaches that assume malicious behaviors to follow predefined profiles and then identify attackers based on such profiles, we consider more practical scenarios that involve various technical challenges:

- **Challenges due to Intelligent Malicious Behaviors**: The design of MBR mechanisms in such a context is particularly challenging as an attacker can act strategically, rather than simply reporting erroneous sensing results to disrupt the final decision. We call such attackers *intelligent malicious users* (IMUs). IMUs can adjust their behavior adaptively to the system's MBR mechanisms to maximize their own utilities, making MBR design and configuration difficult.
- **Challenges due to Lack of Reputation Information**: A widely adopted approach for malicious user detection is based on reputation, which maintains the reputation of each user based on the behavior history. However, reliable reputation information is not always available since well-established historical statistics may be too expensive or even unrealistic in a fast-changing CR environment. The lack of reputation information leads to possible errors in the judgement on

A part of this paper, focusing on the scenarios with only a single malicious user, was presented at IEEE INFOCOM 2014 [1], April 2014.
This work was supported in part by National Natural Science Foundation of China (No. 61261130585), ANR under the grant GreenDyspan (No. ANR-12-IS03), ARO (No. W81NF-12-1-0530), NSF (No. CNS-1160775), SUTD-ZJU Collaboration Research Grant (No. SUTD-ZJU/RES/03/2014) and Open Research Fund of State Key Laboratory of Integrated Services Networks (No. ISN13-08).
Wei Wang is with Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China. (Email: wangw@zju.edu.cn)
Lin Chen is with Laboratoire de Recherche en Informatique (LRI), University of Paris-Sud 11, Orsay 91405, France. (Email: lin.chen@lri.fr)
Kang G. Shin is with Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109-2121, U.S.A. (Email: kgshin@eecs.umich.edu)
Lingjie Duan is with Engineering Systems and Design Pillar, Singapore University of Technology and Design, Singapore. (Email: lingjie_duan@sutd.edu.sg)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

IMUs, thus degrading performance during MBR.

Motivated by the above two design challenges, 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 [10] 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 [11] and design the punishment based on their sensing outcomes. We use exclusion of IMUs from cooperative spectrum sensing and access as a punishment for their malicious behaviors. Specifically, we model MBR with the moral hazard principal-agent framework and design a spectrum sensing and access mechanism with both the participation and the incentive compatibility constraints.
- **Optimal Joint Spectrum Sensing and Access Mechanism**: Without any information on users' reputation, we find that joint spectrum sensing and access are required to thwart the malicious behaviors of both rational and irrational IMUs. By analyzing the resistance cost of MBR methods, we derive the conclusion that the MBR via spectrum sensing can provide an unlimited punishment with resistance cost, while the MBR via spectrum access provides a limited punishment without any resistance cost. We investigate the IMUs' all possible malicious behaviors depending on the penalty factor, which is adopted to minimize the MBR cost. Based on the analysis, we propose optimal joint spectrum sensing and access mechanisms that provide an appropriately moderate incentive to IMUs with the minimum resistance cost.

The rest of this paper is organized as follows. Section 2 introduces our system model and problem formulation and Section 3 models this problem as a principal-agent framework. Section 4 studies the optimal MBR mechanisms against both types of IMUs. Section 5 evaluates the proposed MBR mechanisms by simulation. Possible problem extensions are discussed in Section 6. The related work is discussed in Section 7, and the paper concludes in Section 8.

2 Cooperative Spectrum Sensing Model in the Presence of Malicious Users

We consider a generic model of CR networks consisting of a set $\mathcal{N} = \{1, \cdots, N\}$ of SUs who opportunistically exploit the spectrum of PUs [12], [13]. 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:

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

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 PU 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:

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

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, $\Pr(\mathcal{R}_0^{(i)} | \mathcal{S}_0^{(i)}) = \Pr(\mathcal{R}_1^{(i)} | \mathcal{S}_1^{(i)}) = 1$. Considering the worst case, the IMUs cooperate with each other and deliberately report a false sensing result according to their malicious behavior 'script'. The malicious behaviors are determined to maximize the IMUs' utility. Define M as the number of IMUs. We assume that the number of IMUs is much smaller than that of honest users.

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 PU activities [14]. 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

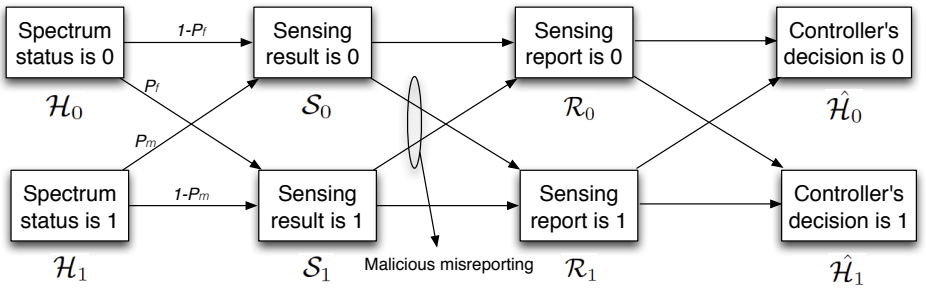


Fig. 1. Cooperative spectrum sensing model with malicious behaviors

To compensate the PU performance degradation caused by the PU-SU collision and provide economic incentives to PUs for spectrum sharing, a penalty [15], [16] would be imposed on the SU system. Let α be the penalty factor of PU–SU collision, capturing the tradeoff between the SU throughput and the impact on the PU system. 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

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

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 PU 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.

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

To motivate all users to report their sensing results honestly, we model secure cooperative spectrum sensing using the moral hazard principal-agent model [10][11], 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 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. Based on the malicious behavior analysis and the principal-agent framework, we would like to design MBR mechanisms to thwart the malicious behaviors of IMUs.

3.1 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 investigate two typical IMUs in this paper according to their motivation.

1) *Rational IMU*: The rational IMUs aim to maximize their own utilities, which is the most common case.
2) *Irrational IMU*: The irrational IMUs aim to cause the most damage possible to the system, which is the worse case.

Both are assumed to have the information of the underlying MBR mechanism and adjust their behaviors intelligently.

For the rational IMUs, the objective is to maximize their effective spectrum resource, which is defined as the accessible spectrum minus the imposed penalty. Note that the rational IMUs may tolerate a higher cost for malicious behaviors than the honest users. We use $\eta \in (0,1]$ as the coefficient of the penalty tolerance for rational IMUs, i.e., the penalty weights for rational IMUs are $\alpha\eta$. The objective can be written as

$$\max_{A} \; u(A, \boldsymbol{\rho}), \quad (4)$$

where A is the IMUs' behaviors. The utility $u(A, \boldsymbol{\rho})$ can be achieved in two cases. First, the rational IMUs utilize the allocated channel resource when the controller's decision is $\hat{\mathcal{H}}_0$. Second, the rational IMUs occupy the channel when the controller's decision is $\hat{\mathcal{H}}_1$.

For the irrational IMUs, the objective is to minimize the system utility defined in Eq. (3):

$$\min_{A} \; U(A, \boldsymbol{\rho}). \quad (5)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

Besides the above two cases similar to the rational IMUs, the irrational IMUs have an extra case, which increases the penalty to the system caused by PU–SU collision by cheating from $\mathcal{S}_1$ to $\mathcal{R}_0$. The irrational IMUs do not utilize the channel to transmit data so that the penalty to a single user can be avoided.

The utilities achieved by the rational and irrational IMUs with different sensing and reporting results are provided in [1].

3.2 The Principal-Agent Framework

The principal-agent model [10][11] is an efficient way to motivate the agent to act on behalf of the principal. We consider the following key components of cooperative spectrum sensing in the presence of IMUs in the principal-agent framework.

- *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 IMUs could achieve the benefit of sensing falsification. The falsification benefit of IMUs when choosing A_m is set as a negative cost, i.e., $C_m < 0$.
- *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 penalty by the PU 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. □

3.3 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 doesnt, 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 N-user secondary system with M IMUs to access the spectrum is that the penalty factor α for the PU–SU collision should satisfy

$$\alpha \leq \frac{\Pr(\mathcal{H}_0)}{\Pr(\mathcal{H}_1)} \left(\frac{1 - P_f}{P_m} \right)^{N-M}. \tag{6}$$

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.

$$U = \Pr(\mathcal{H}_0 \hat{\mathcal{H}}_0) - \alpha \Pr(\mathcal{H}_1 \hat{\mathcal{H}}_0). \tag{7}$$

Let's consider the best case when the sensing results from IMUs are just ineffective but do not cause negative effects, then the system utility is

$$U = \Pr(\mathcal{H}_0)(1 - P_f)^{N-M} - \alpha \Pr(\mathcal{H}_1) P_m^{N-M} \geq 0. \tag{8}$$

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 PU system, the lower bound of the penalty factor α should be

$$\alpha > \frac{\Pr(\mathcal{H}_0)}{\eta \Pr(\mathcal{H}_1)}. \tag{9}$$

Proof: To prevent the SUs' unbridled access, the PU system always adjusts the penalty 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.,

$$u = \Pr(\mathcal{H}_0) - \alpha \eta \Pr(\mathcal{H}_1) < 0, \tag{10}$$

so the lemma holds. □

Remark 2 (Feasible Region of α): The above two lemmas provide upper and lower bounds for the penalty 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

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.

4 Optimal Joint Spectrum Sensing and Access for Malicious Behavior Resistance

In this section, we 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 and motivate the IMUs to report the sensing results honestly with the minimum resistance cost by an appropriately moderate incentive. Thus, the SU system can thwart the malicious behaviors successfully and achieve the maximal system utility. The user index i is omitted for simplicity of presentation.

4.1 Thwarting Rational IMUs

Based on the malicious behavior analysis in [1], it is possible for the rational IMUs 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

$$\Pr(\mathcal{H}_0|\mathcal{S}_0) = \frac{\Pr(\mathcal{H}_0)(1-P_f)^M}{\Pr(\mathcal{H}_0)(1-P_f)^M + \Pr(\mathcal{H}_1)P_m^M} \quad (11)$$

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

We investigate the case without MBR to analyze the necessity of MBR.

Lemma 3: Without any MBR mechanism, if the penalty factor α satisfies

$$\alpha < \frac{\Pr(\mathcal{H}_0)(1-P_f)^M(1-(1-P_f)^{N-M}M/N)}{\Pr(\mathcal{H}_1)P_m^M(1-P_m^{N-M}M/N)\eta}, \quad (13)$$

the rational IMUs always report 1 when the sensing result is 0.

Proof: If the rational IMUs report honestly with the sensing result of 0, the expected utility is

$$\begin{aligned} u(A_h) =& \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-M}M/N \\ &- \Pr(\mathcal{H}_1|\mathcal{S}_0)P_m^{N-M}\alpha\eta M/N. \end{aligned} \quad (14)$$

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

$$u(A_m) = \Pr(\mathcal{H}_0|\mathcal{S}_0) - \Pr(\mathcal{H}_1|\mathcal{S}_0)\alpha\eta. \quad (15)$$

The rational IMUs 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. (13), we need to design an MBR mechanism to prevent the malicious behaviors. Let $u(A, \boldsymbol{\rho})$ denote the rational IMUs' 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:

$$N_S = \left(\Pr(\mathcal{H}_0)P_f + \Pr(\mathcal{H}_1)P_m\right)(N-M)\omega_S. \quad (16)$$

Let $\omega_i(t)$ be the exclusion probability in MBR-S for SU i at time slot t, and $\mathcal{M}$ be the set of the IMUs who make falsified reports of sensing results. The following lemma deals with the allocation of exclusion probability over time for a given aggregate exclusion probability.

Lemma 4: Given an aggregate exclusion probability ω_S, different exclusion probability distributions $\omega_i(t)$ achieve the same total utility for the rational IMUs.

Proof: If the rational IMUs cheat from 0 to 1, with the exclusion probability $\omega_i(t)$, the expected utility of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

the rational IMUs in the current slot is

$$\begin{aligned} & u(A_m,(\omega_S,0)) \\ =& \Pr(\mathcal{H}_0|\mathcal{S}_0)\left(\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M}M/N\right. \\ & \left.+(1-\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M})\right) \\ & -\Pr(\mathcal{H}_1|\mathcal{S}_0)\left(\prod_{i\in\mathcal{M}}\omega_i(t)P_m^{N-N_S-M}\alpha\eta M/N\right. \\ & \left.+(1-\prod_{i\in\mathcal{M}}\omega_i(t)P_m^{N-N_S-M})\alpha\eta\right). \end{aligned} \tag{17}$$

Since the system does not have the information on which SUs are IMUs, i.e., the system does not know $\mathcal{M}$, it is impossible for the system to jointly allocate the exclusion probabilities of different SUs to minimize $u(A_m,(\omega_S,0))$. Treating each SU separately, we can find from the above equation that the utility function is linear with respect to $\omega_i(t)$ for a given i. Thus, given an aggregate exclusion probability ω_S, 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 behaviors.

Lemma 5: MBR-S alone cannot prevent the rational IMUs' malicious behaviors.

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

$$\begin{aligned} u(A_h,(\omega_S,0)) =& \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-N_S-M}M/N \\ & -\Pr(\mathcal{H}_1|\mathcal{S}_0)P_m^{N-N_S-M}\alpha\eta M/N. \end{aligned} \tag{18}$$

Because of the participation constraints of SUs, $u(A_h,(\omega_S,0))$ should be larger than 0. When the penalty factor α satisfies Lemma 3, $u(A_m,(\omega_S,0))$ is larger than $u(A_h,(\omega_S,0))$ for small ω_S, and thus larger than 0.

From Eq. (17), $u(A_m,(\omega_S,0))$ is a monotonously increasing function of $\omega_i(t)$. when $u(A_m,(\omega_S,0))>0$, its minimum is achieved when $\omega_i(t)=1$ for all SUs. Comparing Eqs. (17) and (18), the following inequality holds:

$$u(A_h,(\omega_S,0)) \le u(A_m,(\omega_S,0)). \tag{19}$$

Both sides of this inequality are equal only if $\omega_i(t)=1$, $\forall i$.

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 IMUs' utility decreases as the aggregate exclusion probability ω_S increases because its reported result is ignored. With a large enough ω_S, the malicious behaviors 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 6: The upper bound of ω_S in the MBR-S mechanism is

$$\omega_S < \frac{N-M-\log_{\frac{1-P_f}{P_m}}\frac{\alpha\Pr(\mathcal{H}_1)}{\Pr(\mathcal{H}_0)}}{(\Pr(\mathcal{H}_0)P_f+\Pr(\mathcal{H}_1)P_m)(N-M)}. \tag{20}$$

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

$$\begin{aligned} U =& \frac{N-M}{N}\left(\Pr(\mathcal{H}_0)(1-P_f)^{N-N_S-M}\right. \\ & \left.-\alpha\Pr(\mathcal{H}_1)P_m^{N-N_S-M}\right). \end{aligned} \tag{21}$$

The upper bound of ω_S should be satisfied to ensure that the system utility is positive. Therefore, Eq. (20) follows. □

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

Lemma 7: MBR-A alone cannot prevent the rational IMUs' malicious behaviors.

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 IMUs 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 IMUs' utilities for honest and malicious reports are

$$\begin{aligned} u(A_h,(0,\omega_A)) =& \Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-M}M/N \\ & -\Pr(\mathcal{H}_1|\mathcal{S}_0)P_m^{N-M}\alpha\eta M/N, \end{aligned} \tag{22}$$

$$u(A_m,(0,\omega_A)) = \Pr(\mathcal{H}_0|\mathcal{S}_0)-\Pr(\mathcal{H}_1|\mathcal{S}_0)\alpha\eta. \tag{23}$$

The condition of rational IMUs' malicious reporting is

$$u(A_h,(0,\omega_A)) < u(A_m,(0,\omega_A)), \tag{24}$$

which can be rewritten as

$$\alpha < \frac{\Pr(\mathcal{H}_0|\mathcal{S}_0)(1-(1-P_f)^{N-M}M/N)}{\Pr(\mathcal{H}_1|\mathcal{S}_0)(1-P_m^{N-M}M/N)\eta}. \tag{25}$$

It is always satisfied by Lemma 3. □

Based on Lemmas 5 and 7, neither MBR-S nor MBR-A alone can prevent the rational IMUs' malicious behaviors. 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 IMUs can continue to misreport the sensing result and transmit data, possibly achieving more utility than the punishment. Here, we consider the case when the IMUs are cooperative and one of them is selected randomly to misreport the sensing results. Define $\omega_S(t)$ as the average exclusion probability in MBR-S of the IMUs at time slot t. Note that we cannot calculate $\omega_S(t)$ by averaging $\omega_i(t)$ for all IMUs, since the system does

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

not have the information of the set of IMUs. Instead, we obtain $\omega_S(t)$ as follows.

According to Lemma 4, 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

$$\omega_S(t) = \omega_S \Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1)/M. \tag{26}$$

where $\Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1)$ is the probability of the rational IMUs' malicious behaviors.

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

According to these properties, we set ω_A to be large enough since MBR-A incurs no resistance cost but its punishment is upper-bounded. To achieve a low resistance cost, the optimal ω_S is set to adjust the punishment level so that the expected utilities for honest and malicious reports are the same. Thus, we propose a MBR mechanism for thwarting the rational IMUs as Algorithm 1.

Algorithm 1 Optimal MBR Mechanism for Rational IMUs

1) MBR-S: ω_S is searched to satisfy

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)M/N = \Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1)\Delta u(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1), \tag{27}$$

where $\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) = \Pr(\mathcal{H}_0)\omega_S(t)(1-P_f)^{N-N_S-M}$, $\Pr(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1) = (\Pr(\mathcal{H}_0)(1-P_f)^M + \Pr(\mathcal{H}_1)P_m^M)(1-\omega_S(t)(1-P_f)^{N-N_S-M})$, and $\Delta u(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1)$ is the rational IMUs' expected utility of misreporting. Here, $\Delta u(\mathcal{S}_0\mathcal{R}_1\hat{\mathcal{H}}_1) = 1$.

2) MBR-A: ω_A is set as

$$\omega_A = \left\lceil \Pr(\mathcal{H}_0)\omega_S(1-P_f)^{N-N_S-M}/M \right\rceil, \tag{28}$$

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

4.2 Thwarting Irrational IMUs

The irrational IMUs' utility conflicts with the system utility. It is difficult to provide the irrational IMUs 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 IMUs' malicious behaviors.

The basic idea of the optimal MBR mechanism for irrational IMUs is similar to that for rational IMUs, but there exist some differences because of thier different objectives. Also, the irrational IMUs can cheat from $\mathcal{S}_0$ to $\mathcal{R}_1$ and from $\mathcal{S}_1$ to $\mathcal{R}_0$.

Lemma 8: Without any MBR mechanism, the irrational IMUs always report 1 when the sensing result is 0. It reports 0 when the sensing result is 1 if the penalty factor α satisfies

$$\alpha > \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-M}(1-(1-P_f)^M)}{\Pr(\mathcal{H}_1)P_m^{N-M}(1-P_m^M)}. \tag{29}$$

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

$$\begin{aligned} u(A_h) =& \Pr(\mathcal{H}_0|S_0)\Big((1-P_f)^{N-M}\frac{M}{N} \\ &+ (1-(1-P_f)^{N-M})\Big) \\ &+ \Pr(\mathcal{H}_1|S_0)P_m^{N-M}\alpha\frac{N-M}{N}. \end{aligned} \tag{30}$$

The utility for cheating from 0 to 1 is

$$u(A_m) = \Pr(\mathcal{H}_0|S_0). \tag{31}$$

The irrational IMUs report honestly when

$$\alpha > \frac{\Pr(\mathcal{H}_0)(1-P_f)^N}{\Pr(\mathcal{H}_1)P_m^N} \tag{32}$$

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

The irrational IMUs' utility for honestly reporting when the sensing result is 1 is calculated as

$$u(A_h) = \Pr(\mathcal{H}_0|S_1), \tag{33}$$

while that for cheating is

$$\begin{aligned} u(A_m) =& \Pr(\mathcal{H}_0|S_1)\Big((1-P_f)^{N-M}\frac{M}{N} \\ &+ (1-(1-P_f)^{N-M})\Big) \\ &+ \Pr(\mathcal{H}_1|S_1)P_m^{N-M}\alpha\frac{N-M}{N}. \end{aligned} \tag{34}$$

The condition of cheating is

$$\alpha > \frac{\Pr(\mathcal{H}_0|S_1)(1-P_f)^{N-M}}{\Pr(\mathcal{H}_1|S_1)P_m^{N-M}}. \tag{35}$$

The conditional probabilities are

$$\Pr(\mathcal{H}_0|S_1) = \frac{\Pr(\mathcal{H}_0)(1-(1-P_f)^M)}{\Pr(\mathcal{H}_0)(1-(1-P_f)^M) + \Pr(\mathcal{H}_1)(1-P_m^M)}, \tag{36}$$

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

According to the the above conditional probabilities, the condition of cheating can be rewritten as Eq. (29) and the lemma holds. □

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

The following lemma discusses the allocation of exclusion probability over time for a given aggregate exclusion probability, which is similar to that for rational IMUs. The difference is that both types of malicious behavior in Lemma 8 should be considered for irrational IMUs. Note that the utility u of irrational IMUs is also different from its definition for rational IMUs.

Lemma 9: Given an aggregate exclusion probability ω_S, different exclusion probability distributions $\omega_S(t)$ achieve the same total utility for the irrational IMUs.

Proof: If the irrational IMUs cheat only when the sensing results are 0, with the exclusion probability $\omega_i(t)$, the expected utility of the irrational IMUs in the current slot is

$$\begin{aligned} &u(A_m,(\omega_S,0))\\ &=\Pr(\mathcal{H}_0\mathcal{S}_0)\Big(\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M}M/N\\ &\quad+(1-\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M})\Big)\\ &\quad+\Pr(\mathcal{H}_1\mathcal{S}_0)\left(\prod_{i\in\mathcal{M}}\omega_i(t)P_m^{N-N_S-M}\alpha(N-M)/N\right). \end{aligned} \tag{38}$$

If the irrational IMUs would cheat from 0 to 1 and from 1 to 0, the expected utility in the current slot is written as (39).

Similar to the situation of rational IMUs, we can find that the utility function is linear in $\omega_i(t)$ for a given i for both types of malicious behavior of irrational IMUs in Lemma 8 by treating each SU separately. Therefore, this lemma holds. □

Now, we show that neither MBR-S nor MBR-A alone can prevent the irrational IMUs' malicious behaviors effectively.

Lemma 10: MBR-S alone cannot prevent the irrational IMUs' malicious behaviors.

Proof: If the irrational IMUs cheat only when the sensing results are 0, with MBR-S only, the utility of irrational IMUs for reporting honestly is

$$\begin{aligned} u(A_h,(\omega_S,0))=&\Pr(\mathcal{H}_0\mathcal{S}_0)\big((1-P_f)^{N-N_S-M}M/N\\ &+(1-(1-P_f)^{N-N_S-M})\big)\\ &+\Pr(\mathcal{H}_1\mathcal{S}_0)P_m^{N-N_S-M}\alpha(N-M)/N. \end{aligned} \tag{40}$$

Comparing Eqs. (38) and (40), $u(A_h,(\omega_S,0)) = u(A_m,(\omega_S,0))$ is satisfied only when $\omega_i(t)=1$ for all SUs.

$$u(A_h,(\omega_S,0))\le u(A_m,(\omega_S,0)). \tag{41}$$

If $\omega_i(t)=1$ for all SUs at all time, 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. Therefore, it is always satisfied that

$$u(A_h,(\omega_S,0))<u(A_m,(\omega_S,0)). \tag{42}$$

If the irrational IMUs would cheat from 0 to 1 and from 1 to 0, with MBR-S only, the utility of irrational IMUs for reporting honestly is written as (43).

Comparing Eqs. (39) and (43), the first and third terms are the same as those for the cases with only cheating from 0 to 1. Since $0\le\omega_i(t)\le 1$, the second term of Eq. (43) is also equal to or less than that of Eq. (39). Therefore, it is satisfied that $u(A_h,(\omega_S,0))<u(A_m,(\omega_S,0))$. □

Lemma 11: MBR-A alone cannot prevent the irrational IMUs' malicious behaviors when

$$\alpha>\frac{N}{N-M}\frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-M}(1-(1-P_f)^M)}{\Pr(\mathcal{H}_1)P_m^{N-M}(1-P_m^M)} \tag{44}$$

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 IMUs 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.

If the irrational IMUs cheat only when the sensing results are 0, with MBR-A only, the irrational IMUs' utilities for honest and malicious reports are

$$\begin{aligned} &u(A_h,(0,\omega_A))\\ &=\Pr(\mathcal{H}_0\mathcal{S}_0)\big(1-P_f\big)^{N-M}M/N+(1-(1-P_f)^{N-M})\big)\\ &\quad+\Pr(\mathcal{H}_1\mathcal{S}_0)P_m^{N-M}\alpha(N-M)/N, \end{aligned} \tag{45}$$

$$u(A_m,(0,\omega_A))=\Pr(\mathcal{H}_0\mathcal{S}_0). \tag{46}$$

The condition of the irrational IMUs' malicious reporting is

$$u(A_h,(0,\omega_A))<u(A_m,(0,\omega_A)), \tag{47}$$

which can be rewritten as

$$\alpha\Pr(\mathcal{H}_1)P_m^N<\Pr(\mathcal{H}_0)(1-P_f)^N. \tag{48}$$

According to Lemma 1, the irrational IMUs would misreport their sensing results.

If the irrational IMUs would cheat from 0 to 1 and from 1 to 0, with MBR-A only, the irrational IMUs' utilities for honest and malicious reports are

$$\begin{aligned} &u(A_h,(0,\omega_A))\\ &=\Pr(\mathcal{H}_0\mathcal{S}_0)\left(1-P_f\right)^{N-M}M/N+(1-(1-P_f)^{N-M}))\\ &\quad+\Pr(\mathcal{H}_0\mathcal{S}_1)+\Pr(\mathcal{H}_1\mathcal{S}_0)P_m^{N-M}\alpha(N-M)/N, \end{aligned} \tag{49}$$

$$\begin{aligned} &u(A_m,(0,\omega_A))\\ &=\Pr(\mathcal{H}_0\mathcal{S}_0)+\Pr(\mathcal{H}_0\mathcal{S}_1)(1-(1-P_f)^{N-M})\\ &\quad+\Pr(\mathcal{H}_1\mathcal{S}_1)P_m^{N-M}\alpha(N-M)/N. \end{aligned} \tag{50}$$

For the parts with $\mathcal{S}_0$, i.e., the first and third terms of $u(A_h,(0,\omega_A))$ and the first term of $u(A_m,(0,\omega_A))$, the analysis is similar to that of the previous cases with cheating only when the sensing results are 0. For the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

$$\begin{aligned} u(A_m,(\omega_S,0)) =& \Pr(\mathcal{H}_0\mathcal{S}_0)\left(\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M}M/N+(1-\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M})\right)\\ &+\Pr(\mathcal{H}_0\mathcal{S}_1)\left((1-P_f)^{N-N_S-M}M/N+(1-(1-P_f)^{N-N_S-M})\right)\\ &+\Pr(\mathcal{H}_1\mathcal{S}_0)\left(\prod_{i\in\mathcal{M}}\omega_i(t)P_m^{N-N_S-M}\alpha(N-M)/N\right)+\Pr(\mathcal{H}_1\mathcal{S}_1)\left(P_m^{N-N_S-M}\alpha(N-M)/N\right). \end{aligned} \tag{39}$$

$$\begin{aligned} u(A_h,(\omega_S,0)) =& \Pr(\mathcal{H}_0\mathcal{S}_0)\left((1-P_f)^{N-N_S-M}M/N+(1-(1-P_f)^{N-N_S-M})\right)\\ &+\Pr(\mathcal{H}_0\mathcal{S}_1)\left(\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M}M/N+(1-\prod_{i\in\mathcal{M}}\omega_i(t)(1-P_f)^{N-N_S-M})\right)\\ &+\Pr(\mathcal{H}_1\mathcal{S}_0)P_m^{N-N_S-M}\alpha(N-M)/N. \end{aligned} \tag{43}$$

parts with $\mathcal{S}_1$, the condition of the irrational IMUs' malicious reporting is

$$\begin{aligned} \Pr(\mathcal{H}_0\mathcal{S}_1) <& \Pr(\mathcal{H}_0\mathcal{S}_1)(1-(1-P_f)^{N-M})\\ &+\Pr(\mathcal{H}_1\mathcal{S}_1)P_m^{N-M}\alpha(N-M)/N. \end{aligned} \tag{51}$$

By simplifying the above inequality, Eq. (44) can be obtained. □

The MBR-A decreases the the irrational IMUs' utility when they cheat from 1 to 0 and the spectrum status is $\mathcal{H}_0$, since no spectrum hole would be allocated to the IMUs. Note that the possibility that the MBR-A alone can affect is very small, since the threshold of α in Lemma 11 is almost the same as that in Lemma 8 as N is usually much larger than M.

Based on Lemmas 10 and 11, neither MBR-S nor MBR-A alone can prevent the irrational IMUs' malicious behaviors. Therefore, it is necessary to adopt both MBR-S and MBR-A to design a joint spectrum sensing and access mechanism.

We judge whether or not the two types of misreporting exist by the penalty factor α according to Lemma 8 as

- *Regime* $\mathcal{A}_I$: The penalty factor α satisfies $\frac{\Pr(\mathcal{H}_0)}{\Pr(\mathcal{H}_1)} < \alpha \leq \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-M}(1-(1-P_f)^M)}{\Pr(\mathcal{H}_1)P_m^{N-M}(1-P_m^M)}$. The irrational IMUs would possibly report $\mathcal{R}_1$ when the sensing result is $\mathcal{S}_0$.
- *Regime* $\mathcal{B}_I$: The penalty factor α satisfies $\frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-M}(1-(1-P_f)^M)}{\Pr(\mathcal{H}_1)P_m^{N-M}(1-P_m^M)} < \alpha \leq \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-1}}{\Pr(\mathcal{H}_1)P_m^{N-1}}$, In this regime, we must consider both types of misreporting.

Note that the exclusion probability $\omega_S(t)$ for irrational IMUs is

$$\omega_S(t) = \omega_S \Pr(\mathcal{S}_0\mathcal{R}_1)/M, \tag{52}$$

which is different from (26). This is because the irrational IMUs do not have to access the spectrum to obtain the benefit from their malicious behaviors.

To achieve a low resistance cost, we design the optimal MBR mechanisms for both regimes as Algorithm 2.

Algorithm 2 Optimal MBR Mechanism for Irrational IMUs

Regime $\mathcal{A}_I$:
1) MBR-S: ω_S is searched to satisfy

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)M/N = \Pr(\mathcal{S}_0\mathcal{R}_1)\Delta u(\mathcal{S}_0\mathcal{R}_1), \tag{53}$$

where $\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) = \Pr(\mathcal{H}_0)\omega_S(t)(1-P_f)^{N-N_S-M}$, and $\Delta u(\mathcal{S}_0\mathcal{R}_1) = (1-\omega_S(t))\big(\Pr(\mathcal{H}_0|\mathcal{S}_0)(1-P_f)^{N-N_S-M} - \Pr(\mathcal{H}_1|\mathcal{S}_0)P_m^{N-N_S-M}\alpha(N-M)/N\big)$.
2) MBR-A: ω_A is set as

$$\omega_A = \left\lceil \Pr(\mathcal{H}_0)\omega_S(1-P_f)^{N-N_S-M}/M \right\rceil. \tag{54}$$

Regime $\mathcal{B}_I$:
1) MBR-S: ω_S is searched to satisfy

$$\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0)M/N = \Delta\overline{u}, \tag{55}$$

where $\Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) = \Pr(\mathcal{H}_0)\omega_S(1-P_f)^{N-N_S} + \Pr(\mathcal{H}_0)(1-(1-P_f)^M)(1-P_f)^{N-N_S-M}$, and $\Delta\overline{u}$ is the average increased irrational IMUs' utility of misreporting, i.e., $\Delta\overline{u} = (1-\omega_S(t))((\Pr(\mathcal{H}_0\mathcal{S}_0) - \Pr(\mathcal{H}_0\mathcal{S}_1))(1-P_f)^{N-N_S-M} - \Pr(\mathcal{H}_1\mathcal{S}_0)P_m^{N-N_S-M}\alpha(N-M)/N)$.
2) MBR-A: ω_A is set as

$$\omega_A = \lceil \Pr(\mathcal{H}_0\hat{\mathcal{H}}_0) \rceil = 1. \tag{56}$$

4.3 Thwarting Heterogeneous IMUs

We now consider a more practical scenario in which both the rational and irrational IMUs co-exist. The IMUs within the same type cooperate with each other as discussed above, while different types of IMUs determine their malicious behaviors independently due to different objectives (4) and (5) of rational and irrational IMUs. Let M_R and M_I be the numbers of rational and irrational IMUs, respectively.

We analyze the case of heterogeneous IMUs using a three-step approach similar to the case of single-type IMUs considered earlier. The penalty factors α with malicious behaviors are the same as Lemmas 3 and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

8 for rational and irrational IMUs, respectively, since when one type of IMUs deviates from the equilibrium state, they treat other IMUs as honest users. As a result, we can also conclude that neither MBR-S nor MBR-A alone can prevent the malicious behaviors of heterogeneous IMUs.

In the presence of heterogeneous IMUs, we need to classify the value of α to more regimes for identifying possible malicious behaviors. According to the conditions of α in Lemmas 3 and 8, we let $\chi_R = \frac{\Pr(\mathcal{H}_0)(1-P_f)^{M_R}(1-(1-P_f)^{N-M_R}M_R/N)}{\Pr(\mathcal{H}_1)P_m^{M_R}(1-P_m^{N-M_R}M_R/N)\eta}$ and $\chi_I = \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-M_I}(1-(1-P_f)^{M_I})}{\Pr(\mathcal{H}_1)P_m^{N-M_I}(1-P_m^{M_I})}$ for simplicity of expression, and define the regimes as

- *Regime* $\mathcal{A}_H$: The penalty factor α satisfies $\frac{\Pr(\mathcal{H}_0)}{\Pr(\mathcal{H}_1)} < \alpha \leq \min\{\chi_R, \chi_I\}$. Both the rational and irrational IMUs would possibly report $\mathcal{R}_1$ when the sensing result is $\mathcal{S}_0$.
- *Regime* $\mathcal{B}_H$: The penalty factor α satisfies $\chi_R < \alpha \leq \chi_I$. Only the irrational IMUs would possibly report $\mathcal{R}_1$ when the sensing result is $\mathcal{S}_0$.
- *Regime* $\mathcal{C}_H$: The penalty factor α satisfies $\chi_I < \alpha \leq \chi_R$. In this regime, we must consider all of the three types of misreporting.
- *Regime* $\mathcal{D}_H$: The penalty factor α satisfies $\max\{\chi_R, \chi_I\} < \alpha \leq \frac{\Pr(\mathcal{H}_0)(1-P_f)^{N-1}}{\Pr(\mathcal{H}_1)P_m^{N-1}}$. The irrational IMUs would possibly misreport irrespective of the sensing result.

The basic idea in designing the MBR mechanism for heterogeneous IMUs is that the system imposes a large enough punishment against the malicious behaviors to thwart the corresponding IMUs. For reducing the resistance cost, we also adopt the punishment such that the expected utility for honest reporting is equal to the maximum utility for malicious behaviors. We provide the optimal MBR mechanism for heterogeneous IMUs as Algorithm 3.

Algorithm 3 Optimal MBR Mechanism for Heterogeneous IMUs

Regime $\mathcal{A}_H$:
1) MBR-S: Two values of ω_S can be obtained to satisfy (27) with $M = M_R$ and (53) with $M = M_I$, respectively. ω_S is set to the larger value.
2) MBR-A: ω_A is set as

$$\omega_A = \lceil \Pr(\mathcal{H}_0)\omega_S \max\{(1-P_f)^{N-N_S-M_R}/M_R, (1-P_f)^{N-N_S-M_I}/M_I\}\rceil. \quad (57)$$

Regime $\mathcal{B}_H$: The MBR mechanism is the same as that for Regime $\mathcal{A}_I$.

Regime $\mathcal{C}_H$:
1) MBR-S: Two values of ω_S can be obtained to satisfy (27) with $M = M_R$ and (55) with $M = M_I$, respectively. ω_S is set to the larger value.
2) MBR-A: ω_A is set as

$$\omega_A = \lceil \max\{\Pr(\mathcal{H}_0)\omega_S(1-P_f)^{N-N_S-M_R}/M_R, 1\}\rceil. \quad (58)$$

Regime $\mathcal{D}_H$: The MBR mechanism is the same as that for Regime $\mathcal{B}_I$.

5 Performance Evaluation

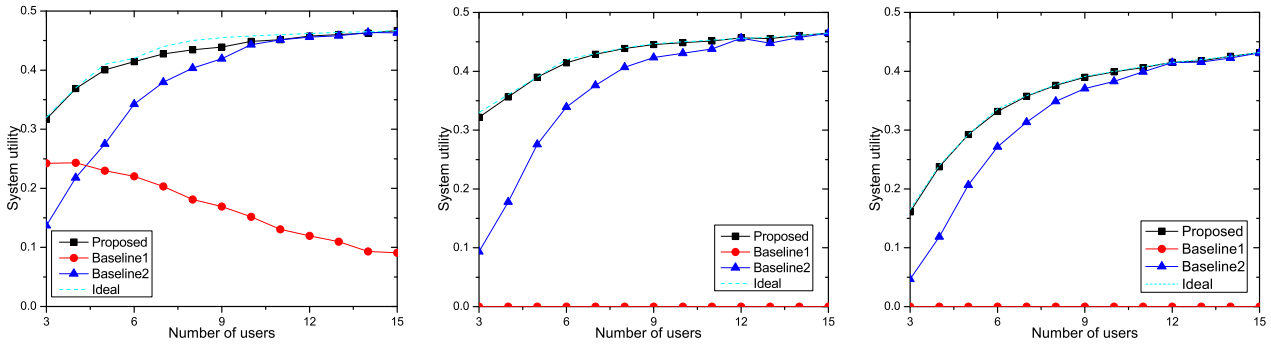
We now evaluate the performance of the proposed MBR mechanisms by simulation. In this simulation, one controller and a number of users are deployed. The sensing results of all users are generated randomly according to the sensing error probabilities P_f and P_m, which are adjusted by the controller to maximize the system utility subject to $P_f + P_m = 0.1$. Then, the IMUs choose their reporting and access behaviors to maximize their utilities, and the controller makes the spectrum sensing and access decisions using the proposed MBR mechanism. The spectrum status is also generated randomly according to $\Pr(\mathcal{H}_0) = \Pr(\mathcal{H}_1) = 0.5$. The penalty factor of PU–SU collision is set to $\alpha = 5$ and $\eta = 1$. To evaluate the average performance, 10000 randomly generated sensing results are considered.

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

- *Ideal sensing*: The controller can detect all false reports of sensing results and equally share the spectrum opportunities among all users.
- *Baseline 1 (Carrot-and-Stick)* [30]: The users stop cooperation when the malicious behaviors are discovered, and resume cooperation after a certain period of time.
- *Baseline 2 (Fixed punishment)* [31]: The fixed values of the aggregate exclusion probability ω_S are used to exclude the IMUs from cooperative sensing. In this baseline, ω_S is set to 10.

The results in Fig. 2 indicate that the proposed MBR mechanism achieves almost the same performance as the ideal sensing scheme, which can be considered as the performance upper bound. In [31], 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 to the system. Considering the resistance cost, a large cost is incurred if ω_S is large, and the malicious behaviors cannot be prevented if ω_S is small. Therefore, the proposed MBR mechanism optimizes the punishment as an appropriate moderate value and thus, outperforms the fixed punishment scheme. Both the proposed MBR and the fixed punishment schemes provide a large system utility when the users are many. However, the system utility with Carrot-and-Stick scheme decreases with the increasing of number of users. The Carrot-and-Stick scheme does not perform well without accurate reputation metrics, because

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing



(a) A rational IMU (b) An irrational IMU (c) A rational IMU and an irrational IMU

Fig. 2. Performance comparison with different total number of users

all users stop cooperation in the presence of malicious behaviors. Although it thwarts the malicious behaviors of rational IMUs 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 further investigate the key parameter in our proposed mechanism, the aggregate exclusion probability ω_S, to analyze its effects on the system utility, as plotted in Fig. 3. Here, we consider a simple scenario with 5 users ($N = 5$) one of whom is malicious ($M = 1$) to give some insights. As ω_S increases, the utility of the IMUs decreases, demonstrating that the proposed MBR mechanism can reduce the IMUs' utility. There is a jump when ω_S is small in the system utility curve: a result of the IMUs' stop of dishonest reports. With an increasing ω_S, the system can provide more effective resistance to the malicious behaviors, 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 rational IMUs increases the system utility significantly, while the improvement at the jump point for irrational IMUs is not so obvious. This is because the controller has the incentive compatible MBR mechanism with the rational IMUs, and has the opposite objective to the irrational IMUs. From this analysis, we can find that the jump point occurs at the optimal ω_S in the MBR mechanism, where the maximal system utility is achieved.

Fig. 4 shows the optimal ω_S is decreasing in the penalty factor α and increasing in the number of users N. As the penalty factor α gets larger, the required ω_S for thwarting the malicious behaviors is smaller, because a large penalty factor increases the IMUs' risk to be punished with a higher probability due to the PU–SU collision. Fig. 4(b) shows that the penalty factor α has little effect on the optimal value of ω_S. The irrational IMUs just report false sensing results but does not transmit over the spectrum holes, thus avoiding the penalty risk of PU–SU collision. In fact, the optimal ω_S would decrease if α is large enough. According to the conditions of the irrational IMUs' malicious behaviors in Lemma 8, 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 IMUs is larger for a larger number of users.

6 Implementation Considerations

The proposed MBR mechanism provides a principle-agent-based joint spectrum sensing and access framework to incentivize the IMUs to report the sensing results honestly. We now integrate the MBR mechanism into the practical cooperative sensing process.

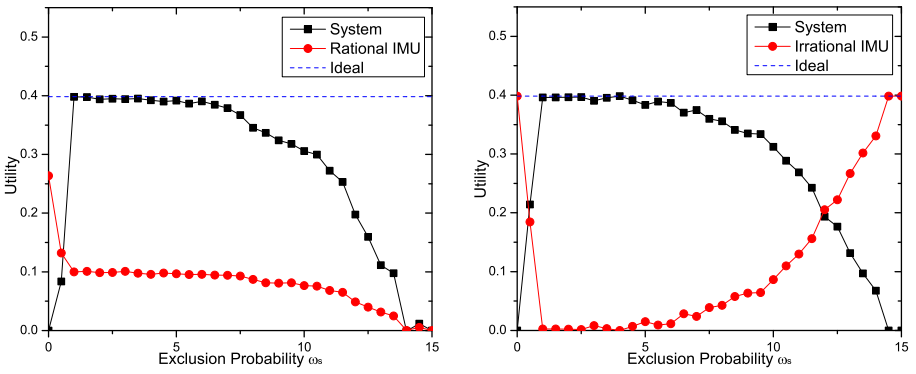
Before the cooperative sensing starts, the controller needs to collect a number of parameters for computing the MBR mechanism: 1) the statistics of channel availability, sensing errors and malicious users are obtained from the historical data or PU spectrum database; 2) the penalty factor α can be told by the PU system; 3) the coordination between the controller and SUs is needed to obtain N and synchronize their sensing, reporting, and decision process.

During the spectrum sensing and access, the controller identifies the suspicious users based on the reported sensing results. As a result, the user identification information should be included in the sensing reporting message. Note that identifying the suspicious users is much easier than identifying the malicious users, which notably facilitates the implementation.

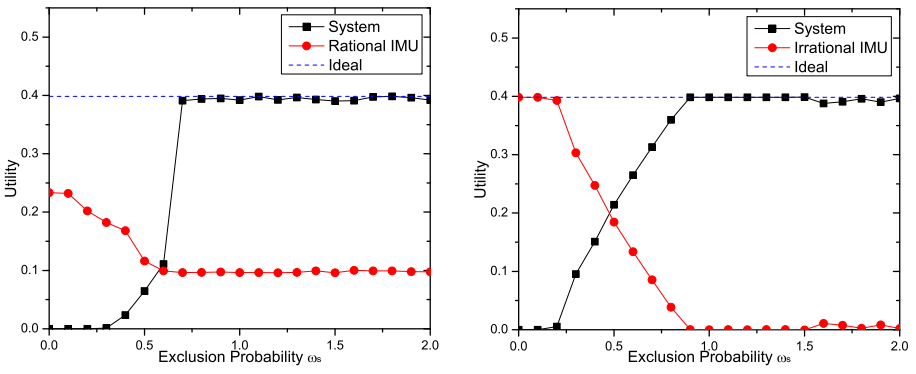
After the spectrum sensing and access, if the PU–SU collision occurs, the SUs who cause the collision share the penalty to compensate the PU system. An economic penalty is becoming a wide-used approach to encourage spectrum sharing [15][16].

From the above discussion, we obtain that the proposed MBR mechanism needs only some trivial modifications on protocols. Furthermore, we want to highlight that the framework can handle more complicated scenarios with incomplete information by slight modifications.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

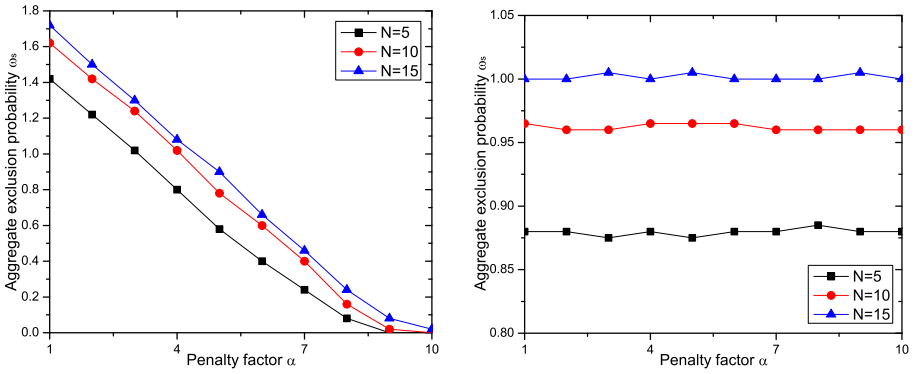


(a) Rational IMUs ($0 \leq \omega_S \leq 15$) (b) Irrational IMUs ($0 \leq \omega_S \leq 15$)



(c) Rational IMUs ($0 \leq \omega_S \leq 2$) (d) Irrational IMUs ($0 \leq \omega_S \leq 2$)

Fig. 3. Effect of the aggregate exclusion probability ω_S



(a) Rational IMUs (b) Irrational IMUs

Fig. 4. Optimal aggregate exclusion probability ω_S

Unknown Type of Malicious Users: The proposed framework can be applied to other types of malicious user by adjusting the parameters of MBR mechanisms if the characteristics of the malicious users are known. For an unknown-type malicious user, the MBR mechanisms for irrational IMUs can be used, although it may conservatively cause a little bit higher resistance cost than that in the cases with the known-type malicious user. In addition, possible malicious behaviors can be judged according to the properties of the penalty factor α. The MBR mechanism is designed just for thwarting possible malicious behaviors with a relatively low resistance cost.

Unknown Number of Malicious Users: If the number of IMUs is known, we can design the MBR mechanism to provide an appropriately large incentive by using the approach in this paper. Without the information about the number of IMUs, however, it is difficult to design a MBR mechanism with an exact appropriate resistance cost. One solution is learning from the feedback of current mechanism [17]. The aggregate exclusion probability ω_S can be set as an upper bound first according to Lemma 6. The parameter decreases step by step and finally approaches the optimal value based on the achieved system utility. For the case when ω_S in Lemma 6 is not large enough, the con-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

troller cannot thwart the malicious behaviors when the participation constraint is met. This is reasonable because it is difficult for the controller to identify the suspicious users correctly in the presence of too many IMUs.

7 Related Work

Secure cooperative spectrum sensing has been studied as a key technology for reliable detection of PUs in CR networks [18]. In [19], a robust reputation-based fusion scheme for sensing data is proposed based on the Byzantine failure model. In [20], the "trust factor" is adopted for each SU based on their reported sensing results. In [21], the reputation-based scheme is investigated with the assistance of some trusted users. As mentioned earlier, such a scheme takes a long time to collect information and build a reliable reputation. Other researchers focused on the detection of attackers. In [22], a malicious user is detected based on SUs' sensing correction with a similar channel fading effect. In [23], the effect of information asymmetry between the attackers and the system is analyzed for independent and dependent attacks. These threshold-based attacker detection schemes cannot prevent the malicious behaviors if the malicious users are intelligent, for example, adopting an attack-and-run strategy. Besides the threshold-based detection, the abnormal statistical sensing behaviors are identified using the hidden Markov model in [24] and the iterative expectation maximization in [25], which also need a long time to collect information. In [26], an extra sensing test is launched to detect malicious users.

An incentive-based economic understanding [27], [28] of attack rationality and benefits is more effective in cooperative sensing, which does not require to differentiate honest users from malicious ones. In [29], the incentive design is combined with the key to motivate the users to sense. In [30], all users stop spectrum sensing if some selfish user deviates from the cooperation "standard". Using a repeated game model, the selfish users are "forced" to cooperate. In [31], direct and indirect punishment strategies are proposed for attack prevention. The malicious users are detected by the PU–SU 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 irrational IMUs who do not access the spectrum for transmission. When malicious users cannot be detected deterministically, the punishment by adjusting the cooperative spectrum sensing strategy is ineffective in preventing the malicious behaviors because of its resistance cost. By adopting a moral hazard principal-agent model, we consider spectrum access together with spectrum sensing to effectively thwart the malicious behaviors of IMUs.

8 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 behaviors of both types of IMUs, we explored the properties of the penalty factor of PU–SU 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] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Secure cooperative spectrum sensing and access against intelligent malicious behaviors," *Proc. IEEE INFOCOM 2014*, Apr. 2014
[2] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," *Proc. IEEE DySPAN 2005*, pp. 131–136, Nov. 2005
[3] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phy. Commun.*, vol. 4, no. 1, pp. 40–62, Mar. 2011
[4] K. G. Shin, H. Kim, A. Min, and A. Kumar. "Cognitive radios: From concept to reality," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 64–74, Dec. 2010
[5] W. Wang, K. G. Shin, and W. Wang, "Joint spectrum allocation and power control for multi-hop cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 7, pp. 1042–1055, Jul. 2011
[6] W. Wang, K. G. Shin, and W. Wang, "Distributed resource allocation based on queue balancing in multi-hop cognitive radio networks," *IEEE/ACM Trans. Netw.*, vol. 20, no. 3, pp. 837–850, Jun. 2012
[7] R. Chen, J. M. Park, and Y. T. Hou, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008
[8] S. Anand, Z. Jin, and 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
[9] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1850 - 1860, Nov. 2012
[10] J. Laffont and D. Martimort, *The Theory of Incentives I: The Principal-Agent Model*, Princeton University Press, Princeton NJ, U.S., 2001
[11] P. Bolton and M. Dewatripont, *Contract Theory*, MIT Press, Dec. 2004
[12] X. Chen and J. Huang, "Evolutionarily Stable Spectrum Access," *IEEE Trans. Mobile Comput.*, vol. 12, no. 7, pp. 1281–1293, Jul. 2013
[13] X. Chen and J. Huang, "Database-assisted Distributed Spectrum Sharing," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2349–2361, Nov. 2013
[14] A. Ghasemi and E. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *J. Commun.*, vol. 2, no. 2, pp. 71–82, Mar. 2007
[15] J. Huang, R. A. Berry, and M. L. Honig, "Distributed interference compensation for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 5, pp. 1074–1084, May 2006
[16] S. Huang, X. Liu, and Z. Ding, "Optimal sensing-transmission structure for dynamic spectrum access," *Proc. of IEEE INFOCOM 2009*, Apr. 2009
[17] X. Cao, *Stochastic Learning and Optimization: A Sensitivity-Based Approach*, Springer, 2007

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2015.2398446, IEEE Transactions on Mobile Computing

[18] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Commun.*, vol.19, no. 6, pp. 106–112, Dec. 2012
[19] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *Proc. of IEEE INFOCOM 2008*, Apr. 2008
[20] P. Kaligineedi, M. Khabbazian, V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," *Proc. of IEEE ICC 2008*, Jun. 2008
[21] K. Zeng, P. Pawelczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Letters*, vol. 14, no. 3, pp. 226–228, Mar. 2010
[22] A. W. Min, K. G. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," *Proc. of IEEE ICNP 2009*, Oct. 2009
[23] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," *Proc. of IEEE DySPAN 2010*, Apr. 2010
[24] X. He, H. Dai, and P. Ning, "HMM-based malicious user detection for robust collaborative spectrum sensing," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2196–2208, Nov. 2013
[25] E. Soltanmohammadi and M. Naraghi-Pour, "Fast detection of malicious behavior in cooperative spectrum sensing," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 377–386, Mar. 2014
[26] T. Bansal, B. Chen, and P. Sinha, "FastProbe: Malicious user detection in cognitive radio networks through active transmissions," *Proc. of IEEE INFOCOM 2014*, Apr. 2014
[27] F. Wu, T. Chen, S. Zhong, L. E. Li, and Y. R. Yang, "Incentive-compatible opportunistic routing for wireless networks," *Proc. of ACM Mobicom 2008*, Sept. 2008
[28] T. Yu, Z. Zhou, D. Zhang, X. Wang, Y. Liu, and S. Lu, "INDAPSON: An incentive data plan sharing system based on self-organizing network," *Proc. of IEEE INFOCOM 2014*, Apr. 2014
[29] S. Li, H. Zhu, Z. Gao, X. Guan, and K. Xing, "YouSense: Mitigating entropy selfishness in distributed collaborative spectrum sensing," *Proc. of IEEE INFOCOM 2013*, Apr. 2013
[30] C. Song and Q. Zhang, "Achieving cooperative spectrum sensing in wireless cognitive radio networks," *ACM Mob. Comput. Commun. Rev.*, vol. 13, no. 2, pp. 14–25, Apr. 2009
[31] L. Duan, A. Min, J. Huang, and 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

Wei Wang received the B.S. degree and the Ph.D. degree from Beijing University of Posts and Telecommunications, China in 2004 and 2009, respectively. Now, he is an associate professor with Department of Information Science and Electronic Engineering, Zhejiang University, China. From Sept. 2007 to Sept. 2008, he was a visiting student with University of Michigan, Ann Arbor, USA. From Feb. 2013 to Feb. 2015, he was a Hong Kong Scholar with Hong Kong University of Science and Technology, Hong Kong. His research interests mainly focus on cognitive radio networks, green communications, and radio resource allocation for wireless networks.

He is the editor of the book "*Cognitive Radio Systems*" (Intech, 2009) and serves as an editor for *Transactions on Emerging Telecommunications Technologies (ETT)*. He serves as TPC co-chair for CRNet 2010 and NRN 2011, symposium co-chair for WCSP 2013, tutorial co-chair for ISCIT 2011, and also serves as TPC member for major international conferences.

Lin Chen received his B.E. degree in Radio Engineering from Southeast University, China in 2002 and the Engineer Diploma from Telecom ParisTech, Paris in 2005. He also holds a M.S. degree of Networking from the University of Paris 6. He currently works as associate professor in the department of computer science of the University of Paris-Sud. His main research interests include modeling and control for wireless networks, distributed algorithm design and game theory.

Kang G. Shin is the Kevin & Nancy O'Connor Professor of Computer Science in the Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor. His current research focuses on QoS-sensitive computing and networking as well as on embedded real-time and cyber-physical systems.

He has supervised the completion of 75 PhDs, and authored/coauthored more than 830 technical articles, a textbook and more than 30 patents or invention disclosures, and received numerous best paper awards, including the Best Paper Awards from the 2011 ACM International Conference on Mobile Computing and Networking (MobiCom11), the 2011 IEEE International Conference on Autonomic Computing, the 2010 and 2000 USENIX Annual Technical Conferences, as well as the 2003 IEEE Communications Society William R. Bennett Prize Paper Award and the 1987 Outstanding IEEE Transactions of Automatic Control Paper Award. He has also received several institutional awards, including the Research Excellence Award in 1989, Outstanding Achievement Award in 1999, Distinguished Faculty Achievement Award in 2001, and Stephen Attwood Award in 2004 from The University of Michigan (the highest honor bestowed to Michigan Engineering faculty); a Distinguished Alumni Award of the College of Engineering, Seoul National University in 2002; 2003 IEEE RTC Technical Achievement Award; and 2006 Ho-Am Prize in Engineering (the highest honor bestowed to Korean-origin engineers).

He was a co-founder of a couple of startups and also licensed some of his technologies to industry.

Lingjie Duan received the PhD degree from The Chinese University of Hong Kong in 2012. He is an assistant professor in the Engineering Systems and Design Pillar, Singapore University of Technology and Design (SUTD). During 2011, he was a visiting scholar in the Department of EECS at the University of California at Berkeley. His research interests include network economics, resource allocation, and energy harvesting. He is the Finalist of Hong Kong Young Scientist Award 2014, and is the awardee of CUHK Global Scholarship for Research Excellence in 2011. He is now leading the Network Economics and Optimization Lab at SUTD. He serves as a TPC Co-Chair of INFOCOM2014 Workshop on GCCCN, Program Co-Chair of the ICCS2014 special issue on Economic Theory and Communication Networks, and the Wireless Communication Systems (WCS) Symposium Co-Chair of IEEE ICCC 2015. He is also a TPC member for many top-tier conferences.