Incentivize Cooperative Sensing in Distributed Cognitive Radio Networks with Reputation-based Pricing

Tongjie Zhang, Zongpeng Li, Reihaneh Safavi-Naini
Department of Computer Science, University of Calgary
{tozhang, zongpeng, rei}@ucalgary.ca

***Abstract*—In a cognitive radio network, selfish secondary users may not voluntarily contribute to desired cooperative sensing. We design the first fully distributed scheme to incentivize participation of nodes in cooperative sensing, by connecting sensing and spectrum allocation, and offering incentive from latter to the former. Secondary users that are more active and report more accurate sensing values will be given higher reputation values, which results in lower prices in the spectrum allocation phase. Theoretical analysis and simulation results indicate that the proposed method effectively incentivizes sensing participation, and rewards truthful and accurate reporting. Our proposed system is fully distributed and does not rely on a central authority, and so is more applicable in dynamic cognitive radio networks in practice. We also show how to improve the robustness of reputation when malicious nodes report spurious reputation.**

***Index Terms*—Cognitive Radio Networks; Cooperative Sensing; Reputation; Spectrum Allocation; Incentive; Pricing**

I. Introduction

As wireless devices and applications proliferate, spectrum frequency becomes a scarce resource. *Cognitive Radio Network (CRN)* is envisioned as an intelligent wireless communication system that can mitigate such spectrum scarcity problem [19]. In CRNs, the unlicensed users (secondary users) can lease spectrum from the license holders (primary users) if no harmful interference is incurred to the latter. Compared to the traditional fixed, static spectrum allocation, CRNs bring more efficient usage of radio frequency for wireless communication [19]. To minimize the potential interference with the primary users, secondary users first sense whether the spectrum of interests are occupied before attempting to access it.

It is challenging for a single secondary user to carry out reliable and accurate spectrum sensing, since wireless signals suffer from fading, noise and interference, which degrade the sensing accuracy of a secondary user. Cooperative sensing is proposed to achieve more accurate decision-making, reduce amortized resource consumption at individual nodes, improve the throughput, and overcome the performance degradation. Cooperative sensing enables multiple secondary users to collaborate with each other in the spectrum sensing process [19]. If the group decision on the spectrum state indicates that the primary users are idle, then the secondary users apply spectrum allocation protocols to decide which of them may access the fallow spectrum.

Cooperative sensing protocols are subject to *Spectrum Sensing Data Falsification (SSDF)* attacks, where the adversary corrupts a subset of secondary users to report falsified sensing results, aiming to degrade the final group decision. A series of studies in the literature propose methods to improve sensing accuracy by counter-measuring SSDF attacks. These solutions are usually based on a centralized infrastructure, where a central authority plays an essential role in coordinating the attack defending. However, the centralized methods usually incur heavy communication overhead between the central authority and the cognitive radios. The adversary can even aim to compromise the central authority, a single point of failure whose capturing may paralyze the entire network. The cost of constructing an infrastructure is also high. It is desirable to design secure, scalable, and distributed schemes in CRNs without a central authority. However, the removal of the central authority brings a number of new challenges. A recent work introduces the distributed method to help secondary users obtain more accurate cooperative sensing results through an iterative update algorithm [13].

Another problem in a CRN is the existence of selfish secondary users. Not all secondary users are willing to participate in the cooperative sensing process, which requires individual sensing and interaction with neighboring nodes, and hence consumes energy and CPU cycles. In distributed CRNs, the secondary users may belong to different operators with different base stations, potentially pursuing selfish goals and making independent decisions towards whether to cooperate with other secondary users, to act alone, or even to become a free-rider. To implement fairness in the network and help honest secondary users obtain better sensing results, effective control of such selfish behaviour is important. How to incentivize the non-malicious but selfish secondary users to participate in the cooperative sensing process is therefore an interesting and important topic to investigate.

The incentivizing method for cooperative sensing also needs to be fully distributed without a central authority. We model the spectrum sensing and spectrum allocation processes as a non-cooperative game. In our system, the reputation values that reflect the sensing participation and the sensing accuracy are used to offer incentive in the pricing function used in the spectrum allocation process. To obtain a lower price for utilizing fallow spectrum, a secondary user needs to participate

This work was supported in part by NSERC (Natural Sciences and Engineering Research Council of Canada) and AITF (Alberta Innovates Technology Futures).

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

more in the spectrum sensing process, and report accurate sensing reports. We propose the method to calculate global reputation values for the secondary users, that can incentivize them to participate in the cooperative sensing processes with more accurate results on more channels. In the reputation fusion process, the adversary may also compromise some secondary users to report spurious reputation values, aiming to improve their pricing factors in the spectrum allocation process. We also design a distributed algorithm to countermeasure this kind of attacks.

The main contributions of this paper are summarized below.

(1) This work is the first to address the problem of incentivizing cooperation in spectrum sensing together with the spectrum allocation process. We design a reputation-based pricing method to offer strong incentive for secondary users to pursue a lower price in the spectrum allocation process. Such connection brings more effective incentives for secondary users to participate in the cooperative sensing process, compared to offering incentives from spectrum sensing only.

(2) We consider two factors of generating reputation for secondary users, both from sensing participation and from sensing accuracy. This method can better reflect the real world nature of communication networks, and countermeasure SSDF attacks from malicious nodes. Secondary users are not only incentivized to participate in the sensing in more channels, but also to report more accurate measurement results.

(3) We design the first fully distributed algorithm to help secondary users compute the global reputation value on sensing accuracy as public knowledge. Secondary users iteratively update their local reputation values to arrive at consensus, without help from any central authority, for the global reputation value.

(4) To countermeasure attacks in the reputation fusion process with spurious reputation from malicious nodes, we design the first fully distributed algorithm to improve the robustness of reputation. The accuracy of the public knowledge is improved, therefore, the incentives are more robust for non-malicious but selfish secondary users.

In the rest of the paper, Sec. II reviews related work, Sec. III introduce the network model and attack model. Sec. IV discusses the selfish behaviors. Sec. IV presents the reputation-based pricing method. Sec. VI is on reputation generation, and Sec. VII is on defending attacks in the reputation generation process. Sec. VIII presents simulation results. Sec. IX concludes the paper.

II. Related Work

Selfishness in collaborative sensing has recently attracted much attention. Song *et al.* first studied this problem and proposed incentive strategies [15]. Mukherjee further discussed this problem in a partially-connected network with imperfect information [2]. However, both work consider only the utility (payoff) function for secondary users as improved sensing accuracy compared to individual sensing, which is only from the spectrum sensing process. Wang *et al.* studied how secondary users can collaborate through an evolutionary game [16]. A recent work considers another selfish behavior where secondary users report arbitrary information as their sensing results or simply copy other secondary users' reports, to save the sensing energy [17]. However, both work only consider hard fusion with binary results of the primary user state, which is less fine-grained compared to soft fusion where real values from the sensed information of the primary users are exchanged. El-Sherif *et al.* discussed the joint design of spectrum sensing and spectrum allocation [23], but only considered individual spectrum sensing without cooperation.

For cooperative sensing without a central authority, Li *et al.* first proposed to remove the fusion center by enabling all cognitive radios to update their local measurements with neighbouring nodes iteratively towards consensus [14]. Each secondary user obtains local measurements of the primary user signals and then exchanges only with its neighbours. A secondary user updates its value based on its own value and the received values from all its neighbours. The updated values are then exchanged iteratively, until a consensus is reached among all secondary users [18]. To countermeasure SSDF attacks in a distributed CRN, a recent work uses reputation to improve the cooperative sensing accuracy [13].

There are a number of models for spectrum allocation. Some models assume that there exists a central authority that controls and coordinates the spectrum allocation [3]–[5], [7]–[9]. The problem of allocating spectrum based on the *Quality of Service (QoS)* requirements of secondary users have been recently studied [3]–[5]. Some secondary users require minimum-rate guaranteed services such as *Voice over IP (VoIP)*, while some secondary users only require best effort service such as WiFi data services. These works all assume a single base station as the central authority to allocate spectrum resources to secondary users. A number of solutions propose distributed spectrum allocation methods [10]–[12], where each secondary user makes its own decision about the spectrum access strategy, mainly based on local observation of the spectrum dynamics. A hybrid method, called distributed-centralized spectrum allocation, enables the secondary users to elect a leader randomly from either the secondary users or the primary users to act as the central authority [6].

III. System Model

A. Network Model

We consider a hybrid network consisting of several primary user networks and a secondary user network. There are N secondary users. The total radio spectrum consists of K orthogonal frequency channels. Each primary user network operates over one channel. Let $\Omega_N = \{1, 2, \ldots, N\}$ and $\Omega_K = \{1, 2, \ldots, K\}$ denote the sets of secondary users and channels, respectively. Each secondary user is equipped with a cognitive radio. They utilize omnidirectional antennas to communicate with each others. The network formed by the secondary users is modeled as an undirected graph where all secondary users are either directly or indirectly connected. The set of secondary users are the nodes $\mathcal{V}$, and the set of edges is $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$. Two users i and j are neighbours if $(i, j) \in \mathcal{E}$.

$N_i = \{j|(i,j) \in \mathcal{E}\} \subset \mathcal{V}$ is the set of neighbours of i. Secondary users are located within the transmission range of the primary users, and can individually sense the environment to detect the existence of the primary users.

We use the energy sensing method in the cooperative sensing process for a secondary user to detect primary users' presence. An active secondary user measures the primary user energy in a sensing session. Each sensing session is followed by a series of value update sessions, where active secondary users exchange local measurements with neighbors, and update their own values based on received values. For the honest nodes, the initial values are the sensed values of the primary user energy. The malicious nodes may report arbitrary values aiming to achieve their malicious goals.

If the cooperative sensing results indicate that the primary users are not transmitting on certain channels, the secondary users can transmit on these unoccupied channels. The secondary users are able to transmit or receive over multiple channels simultaneously. They can also share a particular channel with different transmission power, which leads to a corresponding level of interference. The transmission power vector of a secondary user i over all channels is denoted by $\mathbf{P}_i = (P_i^1, P_i^2, \ldots, P_i^K)$, where P_i^k is the transmission power of i on channel k. There is an upper limit for the total transmission power of a secondary user over all the channels.

B. Adversary Model

There are three kinds of nodes in the network: (i) always active honest nodes, who participate in all the cooperative sensing processes, and report their sensed results and reputation vectors; (ii) honest but selfish nodes, who may choose not to participate in the cooperative sensing process at all the channels. When they decide to participate, they report their sensed value to neighbors; and (iii) malicious nodes, who may or may not participate in the cooperative sensing process, and report falsified values when participating.

In cooperative sensing, the adversary can be either *selfish*, aiming to have exclusive access to the primary user spectrum, or *vandalic*, aiming to incur severe interferences between the primary users and other secondary users. To achieve these goals, malicious nodes strategically report higher values of the primary users when they are not transmitting, and *vice versa*.

We assume malicious nodes participate in the pricing game with fraudulent information. During the reputation fusion process, malicious nodes may report low reputation values for honest nodes and high reputation values for themselves, aiming at lower prices in the spectrum allocation process.

IV. Selfish Behaviors and Consequences

Secondary users in a distributed CRN are subject to restrictions in weight and form-factor, which in turn limits their power supply. Since frequent battery replacement is not always practical, energy efficiency is in general an important goal. The power consumed by an active sensor is 24 mW compared to merely 0.4 mW by an inactive sensor [1]. As a result, a secondary user has a natural incentive not to sense by itself, but to act as a free-rider by passively receiving the cooperative sensing results from other honest nodes. That is, It can join the network and listen to the communication channel, without implementing the local sensing algorithm. Such selfish behavior has no direct harm to other secondary users. However, the lack of honest neighbors' participations will compromise the level of robustness and accuracy of the cooperative sensing results.

Another reason for selfish behavior of honest secondary users is the energy consumption and delay incurred by the iterative algorithms themselves [2]. Compared with individual sensing, the iterative algorithms proposed in the existing literature delay the decision making process. The cost of additional energy consumption in reporting sensed value to a neighbor is also non-negligible. Weighting the cost and delay from the cooperative sensing process, some honest nodes may choose not to participate in the entire process, but to perform local sensing only. If these secondary users have better sensing technologies by themselves, it makes sense for them not to participate and share their data. Apparently, such selfish behavior also has a negative impact on the overall wellbeing of the distributed CRN.

Our recent work showed that honest secondary users can obtain more accurate cooperative sensing reports in an adversarial environment, as long as more than half of the neighbors correctly report sensed values [13]. This was based on the assumption that all honest secondary neighbors actively participate in the entire cooperative sensing process. However, some honest neighbors may not actively participate in the process. More honest secondary users can help the secondary user network to obtain a more accurate cooperative sensing result. The selfish behaviors of some of the honest nodes however may result in less accurate cooperative sensing results at other secondary users, which will degrade the performance of the distributed cooperative sensing. This loss of accuracy will adversely affect all nodes and in particular the selfish secondary users who will use the cooperative sensing results generated from the active secondary users. This can incentivize the honest secondary users to participate in the cooperative sensing process. However, the incentive from the cooperative sensing process itself does not apply to the cases where honest nodes choose to sense by themselves but not to report.

V. The Incentive Method

To offer stronger incentives for honest nodes to participate in the cooperative sensing process, we connect sensing participation to the reputation in a distributed spectrum allocation process through a user-dependant pricing function in a spectrum allocation game. In the distributed spectrum allocation process, some secondary users behave selfishly to maximize their own performance. A well designed pricing mechanism can elicit social efficient behaviours from them.

We adopt the noncooperative game among secondary users proposed in recent literature [10]. The game $\mathcal{G}$ is expressed as $\mathcal{G} = \{\Omega, \mathcal{P}, \{U_i\}\}$, where $\Omega = \{1, 2, \ldots, N\}$ is a finite set of players; $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_N$ is the action

space with $\mathcal{P}_i$ being the action set for player i; and U_i is the utility function of player i, which depends on the strategies of all players, which are the secondary users. They can select different transmission powers on different channels. Higher transmission powers may bring higher achievable data rate. At the same time, higher prices are also incurred. Secondary users select their transmission powers to maximize their respective utility functions, and under certain conditions, they eventually reach a Nash Equilibrium after a number of iterations [10].

We use α_A to denote the probability when the cooperative sensing result correctly determines that a channel k is unoccupied by the primary user in a sensing session A. The utility function of a secondary user i can be considered as the achievable data rate received by i from the network, $\alpha_A \log_2(1 + \frac{\beta G_{ii}^k P_i^k}{\sum_{j\in\Omega_N, j\neq i} G_{ji}^k P_j^k + M_i^k})$, subtracting the cost associated with the pricing function and the cooperative sensing process. Only when the primary user is not transmitting, the cost brought by the pricing function is incurred for a secondary user who is interested to transmit on this channel. We use a linear pricing mechanism [10] to describe the cost incurred by the pricing function, where the price $\alpha_A \lambda_i^k P_i^k$ increases monotonically with transmission power P_i^k. On each channel k, we denote the cost incurred by cooperative sensing for each secondary user as c_i^k. The total cost C_i from cooperative sensing for a node i depends on the number of channels it senses K_i, $C_i = \sum_{k=0}^{K_i} c_i^k$. The utility function is defined as:

$$\begin{aligned}\tilde{U}_i(\mathbf{P}_i, \mathbf{P}_{-i}) &= \sum_{k\in\Omega_K} \tilde{u}_i(P_i^k) \\ &= \sum_{k\in\Omega_K} u_i(P_i^k) - \sum_{k\in\Omega_K} \alpha_A \lambda_i^k P_i^k - \sum_{k=0}^{K_i} c_i^k \\ &= \sum_{k\in\Omega_K} \alpha_A [\log_2(1 + \frac{\beta G_{ii}^k P_i^k}{\sum_{j\in\Omega_N, j\neq i} G_{ji}^k P_j^k + M_i^k}) - \lambda_i^k P_i^k] - \sum_{k=0}^{K_i} c_i^k \end{aligned} \quad (1)$$

where $\lambda_i P_i^k$ is the user-dependent linear pricing function that can drive the Nash Equilibrium close to a Pareto optimal solution. G_{ii}^k is the channel gain on channel k of the source to an intended destination, G_{ji}^k is the interference power received at the secondary user i from unintended user j, M_i^k is the noise at i, β is the gap of *SNR (signal-to-noise-ratio)* that is needed to reach a certain capacity between practical implementation and information theoretical results [20].

The social optimization problem is to maximize a weighted sum of the achievable data rates of all secondary users:

$$\max_{\mathbf{P}} \sum_{i\in\Omega_N} R_i \sum_{k\in\Omega_K} \alpha_A \log_2(1 + \frac{\beta G_{ii}^k P_i^k}{\sum_{j\in\Omega_N, j\neq i} G_{ji}^k P_j^k + M_i^k}) \quad (2)$$

where R_i is the reputation of secondary user i, assigned to i to reward active participation and to punish idle behaviors in the cooperative sensing process. When a secondary user has a better reputation, it shall gain a higher utility in the social optimization problem, and *vice versa*.

We adopt the methodology as in [10] to derive the optimal pricing factor for the secondary users, described in (3) on top of the next page. The calculation for (3) is given in the Appendix. The pricing factor depends on the reputation values of all the secondary users in the network. We can observe that the higher reputation value a node i has, the lower reputation values its neighbors have (including both malicious and selfish secondary users), the lower price i has to pay in the spectrum allocation process. This effect can offer a strong incentive for a secondary user i to improve its reputation.

After receiving transmission power P_i^k, the noise M_i^k from the neighbors, measuring G_{ii}^k and G_{ij}^k from the received signal power, and obtaining the reputation values (Sec. VI), each secondary user first adjusts its liner pricing factor over all channels according to (3), and then determines its best action, including the optimal channel selection and the transmission rate on each channel. The goal of user i is to maximize its individual utility function (1). The same procedure happens at all secondary users in the network. The Pareto optimal Nash Equilibrium is reached when all secondary users converge to the best response. The secondary users can update their best responses according to the best responses of their neighbors iteratively, using Jacobi (parallel), Gauss-Seidel (sequential) schemes [10] or asynchronous schemes [21], [22].

VI. Generate Reputation

When discussing the spectrum allocation game, we established a reputation-based pricing scheme for secondary users to reach Nash Equilibrium. A user with higher reputation is assigned a lower price in the game. The next step is to design an appropriate mechanism for generating reputation.

A. Sensing Participation

A natural way of generating R_i is to make public knowledge secondary user i's sensing participation $R_i^{(SP)}$. $R_i^{(SP)}$ is a parameter relevant to the number of channels a secondary user actively senses in a cooperative sensing session. K_i is observable by the neighbors of i.

We use the percentage of sensed channels of i for the optimization: $R_i^{(SP)} = \frac{K_i}{K}$. The higher $R_i^{(SP)}$ is, the better price i will obtain in the spectrum allocation process, which can be used as an incentive for i to increase K_i by participating in more channels. To calculate K_i, each node in the network monitors its neighbors' activity on channel k. We describe this process in Algorithm 1.

Algorithm 1 Calculating Sensing Participation. (Input: The channels a secondary user j participates in. Output: Reputation about sensing participation $R^{(SP)}$ for all the secondary users.)

1: j participates in a subset of all channels
2: j observes the other participants in every channel
3: **while** There is a secondary user i participating on the same channel **do**
4: j broadcasts its observed channel participation information $K_{j,i}$ for another node i
5: j receives the observed channel participation information $K_{1,i}, K_{2,i}, K_{3,i}, \ldots$ for another node i from its neighbors
6: j calculates $K_i = |K_{1,i} \cup K_{2,i} \cup \cdots \cup K_{j,i} \cup \ldots|$
7: i calculates $R_i^{(SP)} = \frac{K_i}{K}$
8: **end while**

$$\lambda_i^k = -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\partial u_j(P_j^k)}{\partial P_i^k}}{R_i} = \frac{\alpha_A \beta}{R_i \ln 2} \sum_{j\in\Omega_N, j\neq i} \frac{R_j G_{ij}^k P_j^k G_{jj}^k}{(\sum_{i\in\Omega_j, i\neq j} G_{ij}^k P_i^k + M_j^k)(\sum_{i\in\Omega_j, i\neq j} G_{ij}^k P_i^k + M_j^k + \beta G_{jj} P_j^k G_{ij}^k)} \quad (3)$$

	Player 1	Player 2	Player 3
$k=1$	Participate	Participate	
$k=2$		Participate	Participate
$k=3$	Participate	Participate	Participate
$k=4$			Participate
$k=5$	Participate		Participate
$k=6$		Participate	Participate
$k=7$	Participate	Participate	

Fig. 1: Observation on the sensing participations of neighbors

Consider the sensing participation in Fig. 1. Player 1 participates in channels $\{1,3,5,7\}$. Player 2 participates in channels $\{1,2,3,4,5\}$. Player 3 participates in channels $\{2,3,4,5,6\}$. Since channel 4 is only sensed by Player 3, Player 3 has to do individual sensing on channel 4. The activeness of Player 3 on channel 4 is not counted towards its participation in cooperative sensing. To obtain K_i, Players 2 and 3 each observes on the channels where they are active. They each records the other players on a channel: $K_{1,2} = \{1,3,7\}$, $K_{1,3} = \{3,5\}$, $K_{2,1} = \{1,3,7\}$, $K_{2,3} = \{2,3,6\}$, $K_{3,1} = \{3,5\}$, $K_{3,2} = \{2,3,6\}$. They broadcast the observations to neighbors. Each player then calculates the cardinality of the union set for each individual neighbor. $K_1 = |K_{2,1} \cup K_{3,1}| = 4$, $K_2 = |K_{1,2} \cup K_{3,2}| = 5$. In this case, $K_3 = |K_{1,3} \cup K_{2,3}| = 4$ rather than $K_3 = 5$. Hereby, $R_1^{(SP)} = R_3^{(SP)} = \frac{4}{7}$, $R_2^{(SP)} = \frac{5}{7}$.

B. Sensing Accuracy

The above method incentivize users with reputation to participate in channel sensing. Considering that malicious nodes can be active in the cooperative sensing process to achieve their malicious goals, the reputation shall be further improved to reflect the sensing accuracy, besides level of participation.

We improve the sensing accuracy and participation by both identifying falsified sensing reports and incentivizing the participation of honest secondary users. This idea is similar as *Elo* rating system for chess and *ATP (the Association of Tennis Professionals) Rankings* for tennis, where the more an athlete plays, the better an athlete performs, and the higher rating an athlete has. When connecting spectrum sensing with the spectrum allocation process, reputation can reflect both sensing accuracy and sensing participation of the secondary users. If a user participates more actively, or senses and reports the primary user state more accurately, it is assigned a lower price in the spectrum allocation process as a reward.

In a given sensing interval, a secondary user i has m_i neighbors who report falsified values (including attacking malicious neighbors and honest nodes sensing incorrectly due to severe fading or system failure), and n_i neighbors who report correct values (including honest nodes sensing correctly and non-attacking malicious nodes). We use $R_{j,i}^{(SA)k}$ to denote the reputation of transmitter i generated by receiver j to reflect the sensing accuracy of i. Each user j maintains a reputation vector of its neighbors, on a channel k: $\{R_{j,1}^{(SA)k}, R_{j,2}^{(SA)k}, \ldots, R_{j,m_j+n_j}^{(SA)k}\}$. All secondary users update their values and exchange their updated values with their neighbors. $V_{i,j}$ is the value that a transmitter i sends to a receiver j. After the first round of sensing value exchange, an honest node calculates the reputation of its neighbors based on their reported values and its own value. The reputation values reflecting sensing accuracy $R_{j,i}^{(SA)k}$ are generated on channel k as follows:

$$R_{j,i}^{(SA)k} = 2 - \frac{(m_j + n_j + 1)|V_{i,j}^k - \tilde{V}_j^k|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^k - \tilde{V}_j^k|} \quad (4)$$

where $\tilde{V}_j^k = \frac{\sum_{l=1}^{m_j+n_j+1} V_{l,j}^k}{m_j+n_j+1}$ is the average value of all the nodes in the neighborhood on channel k [13]. The value of $R_{j,i}^{(SA)k}$ falls into $[0,2]$.

This reputation generating method can assign reputation $R_{j,i}^{(SA)k} < 1$ for a neighbor that reports falsified values, and $R_{j,i}^{(SA)k} > 1$ reputation for a neighbor that reports correct values, which will help honest nodes obtain better cooperative sensing results than the reputation-less scheme, assuming that the majority of neighbors are either correctly sensing honest nodes or non-attacking malicious nodes [13].

C. Reputation Fusion

Reputation values reflecting sensing accuracy of a secondary user are generated individually by its peers, and are fused into a global reputation value for use in the pricing factor of the spectrum allocation process. The reputation fusion process is a distributed scheme without a central authority. Upon detection of an idling primary user, the secondary users exchange their reputation vectors with each other iteratively towards a converged global reputation. Such agreed-upon reputation values become public knowledge in spectrum allocation.

Inspired by the distributed algorithm for cooperative sensing [14], we design a distributed algorithm for secondary users to achieve consensus on global reputation, as described in Algorithm 2. μ is a discount factor. t indicates the reputation update session.

In the distributed reputation fusion algorithm, the consensus reputation value $R_i^{(SA)k}$ for i on channel k is the average reputation value from all secondary users in the network $R_i^{(SA)k} = \frac{\sum_{j\in\Omega_N, j\neq i} R_{j,i}^{(SA)k}}{N_i}$ [18]. Since a node can sense on multiple channels, the reputation value $R_i^{(SA)}$ about a node i can be described as $\frac{1}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k}$. The higher $R_i^{(SA)k}$ it obtains, the lower price i faces in the spectrum allocation process, which can be used as another incentive for i to contribute more accurate sensing results. This statement

Algorithm 2 Distributed Reputation Fusion Algorithm on Channel k. (Input: Reputation vector of a node j: $R_{j,1}^{(SA)k}, R_{j,2}^{(SA)k}, \ldots, R_{j,i}^{(SA)k}, \ldots, R_{j,m_j+n_j}^{(SA)k}$ and received reputation vectors from j's neighbors. Output: The converged reputation vector.)

1: **while** i is a neighbor of j **do**
2: j receives reputation vectors from a neighbor i: $R_{i,1}^{(SA)k}, R_{i,2}^{(SA)k}, \ldots, R_{i,m_i+n_i}^{(SA)k}$
3: j sends its own reputation vector to a neighbor i: $R_{j,1}^{(SA)k}, R_{j,2}^{(SA)k}, \ldots, R_{j,i}^{(SA)k}, \ldots, R_{j,m_j+n_j}^{(SA)k}$
4: **while** The converged reputation vector is not obtained **do**
5: j updates its reputation vector as

$$R_{j,i}^{(SA)k(t+1)} = R_{j,i}^{(SA)kt} + \sum_{l=0}^{m_j+n_j} \mu(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}) \tag{5}$$

6: **end while**
7: **end while**

also implies that a malicious node is less incentivized to attack with falsified sensing results.

The method of generating and fusing $R_i^{(SP)}$ has been discussed before as $R_i^{(SP)} = \frac{K_i}{K}$, which falls into the range of $[0, 1]$. The two reputation vectors can be linearly combined together with parameters ϵ and η, to form the final global reputation R_i to be used in the pricing factor in the spectrum allocation process. Considering the different value ranges of $R_i^{(SA)}$ and $R_i^{(SP)}$, the global reputation value of node i is:

$$\begin{aligned} R_i &= \epsilon R_i^{(SA)} + 2\eta R_i^{(SP)} \\ &= \epsilon \frac{1}{K_i} \sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} + 2\eta \frac{K_i}{K} \\ &= \frac{\epsilon}{K_i N_i} \sum_{k\in\Omega_K, P_i^k>0} \sum_{j\in\Omega_N, j\neq i} (2 - \frac{(m_j+n_j+1)|V_{i,j}^k - \tilde{V}_j^k|}{\sum_{l=1}^{m_j+n_j+1} |V_{l,j}^k - \tilde{V}_j^k|}) \\ &+ \frac{2\eta K_i}{K} \end{aligned} \tag{6}$$

where $0 < \epsilon < 1, 0 < \eta < 1, \epsilon + \eta = 1$.

D. The Role of Reputation

For the linear combination of $R_i^{(SA)}$ and $R_i^{(SP)}$, we now analyze the effect of the parameters towards incentivizing secondary user participation. In the reputation value R_i, $\frac{2\eta K_i}{K}$ offers incentive for both malicious and honest neighbors, $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k}$ offers incentive to honest neighbors only. To differentiate secondary users in the spectrum allocation process, we propose the requirement that is consistent with the requirement for sensing accuracy. We require that $R_i < 1$ for a malicious neighbor i, $R_i > 1$ for an honest neighbor i.

For an honest neighbor i, the requirement is $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} > \frac{K-2\eta K_i}{K}$. Since $\epsilon + \eta = 1$, the requirement translates to $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} > \frac{K-2\eta K_i}{K(1-\eta)}$. Since $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} > 1$, so an honest node has to meet the requirement of $\frac{K-2\eta K_i}{K(1-\eta)} < 1$ to obtain a reputation value $R_i > 1$. This requirement can be transformed to $K_i > \frac{K}{2}$. Hereby, as long as it participates in more than half of the channels and report correctly sensed values, the requirement is satisfied. In this case, the system can incentivize the honest nodes to participate in at least half of the channels. Again, the more channels it participates in, the lower price it can gain in the spectrum allocation process.

For a malicious neighbor i, the requirement is $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} < \frac{K-2\eta K_i}{K}$. Since $\epsilon + \eta = 1$, the requirement translates to $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} < \frac{K-2\eta K_i}{K(1-\eta)}$. Since $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} < 1$, as long as the malicious node i is active on less than half of the channels, $K_i < \frac{K}{2} \Leftrightarrow \frac{K-2\eta K_i}{K(1-\eta)} > 1$, the requirement is satisfied. In this case, the malicious node is for sure to receive $R_i < 1$, which indicates a higher price in the spectrum allocation process.

For an active malicious neighbor i that attacks in more than half of the channels $K_i > \frac{K}{2}$, we need to analyze the effect of parameter η. We can observe that the more channels i actively attacks, the lower $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k}$ is. At the same time, the lower $\frac{K-2\eta K_i}{K(1-\eta)}$ also turns to be. In the extreme situation where the malicious nodes attack all channels, $K_i = K$. The requirement for $R_i < 1$ turns to be $\frac{\epsilon}{K_i}\sum_{k\in\Omega_K, P_i^k>0} R_i^{(SA)k} < \frac{1-2\eta}{1-\eta}$, where $\frac{1-2\eta}{1-\eta}$ is the lower bound for the system to meet the requirement.

VII. Improve the Robustness of Reputation

Malicious nodes are interested in manipulating the reputation values to give themselves lower prices, while give higher prices to honest nodes. Once fused with correct data, such spurious data can lead to detrimental, unfair prices. We further assign differentiated weights to the reputation values about sensing accuracy. Such *reputation-of-reputation* serves as *credibility* to help honest nodes obtain more accurate reputation values their neighbours.

An honest node calculates the credibility of its neighbors based on their reported reputation vectors and its own reputation vector after the first round of reputation exchange in Algorithm 2. We use differentiated weight $\omega_{j,i}^{(SA)k}$ to denote the credibility of the transmitter i generated by the receiver j. Then, we can modify (5) to

$$R_{j,i}^{(SA)k(t+1)} = R_{j,i}^{(SA)kt} + \sum_{l=0}^{m_j+n_j} \mu\omega_{j,i}^{(SA)k}(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}). \tag{7}$$

For requirements on $\omega_{j,i}^{(SA)k}$ to guarantee that the reputation fusion in (7) to be better than that in (5), we have:

Proposition. *Assume a node j can assign credibility $\omega_{j,i}^{(SA)k} < 1$ to a neighbor that reports spurious reputation values, and $\omega_{j,i}^{(SA)k} > 1$ to a neighbor that reports correct reputation values. Then j can update the fused reputation value of a neighbor i to a higher reputation value when i reports correct sensing results, and a lower reputation value when i reports falsified sensing results, compared to the reputation fusion process without credibility $\omega_{j,i}^{(SA)k}$.*

Proof: Let s_i be the number of i's neighbors who transmit spurious reputation, c_i be number of other neighbors. For an honest node j, we denote the credibility of a neighbor i that

reports a correct reputation with $\omega_{j,i_C}^{(SA)k}$, and the credibility of a node i that reports a spurious reputation with $\omega_{j,i_S}^{(SA)k}$. Comparing the two reputation update methods (5) and (7), we have $R_{j,i}^{(SA)k(t+1)} = R_{j,i}^{(SA)kt} + \mu[\sum_{i=0}^{s_j} \omega_{j,i_S}^{(SA)k}(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}) + \sum_{i=s_j+1}^{s_j+c_j} \omega_{j,i_C}^{(SA)k}(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt})]$ and $R_{j,i}^{(SA)k(t+1)} = R_{j,i}^{(SA)kt} + \mu[\sum_{i=0}^{s_j}(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}) + \sum_{i=s_j+1}^{s_j+c_j}(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt})]$. Therefore, the difference between these two methods is:

$$\mu[\sum_{i=0}^{s_j}(\omega_{j,i_S}^{(SA)k} - 1)(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt}) + \sum_{i=s_j+1}^{s_j+c_j}(\omega_{j,i_C}^{(SA)k} - 1)(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt})]. \quad (8)$$

We now examine the two scenarios, when (i) an honest node j generates the reputation of a neighbor correctly, or (ii) incorrectly, in which case the effect is the same as a spurious reputation value. In case (i), $R_{j,i}^{(SA)kt} \approx R_{l,i}^{(SA)kt}$ for a neighbor l that also generate a correct reputation value, then the difference between the two methods is approximately $\mu\sum_{i=0}^{s_j}(\omega_{j,i_S}^{(SA)k} - 1)(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt})$. While i reports a correct sensed value, we have $R_{l,i}^{(SA)kt} < R_{j,i}^{(SA)kt}$ for a neighbor l that reports a spurious reputation value. So, as long as $\sum_{i=0}^{s_j}(\omega_{j,i_S}^{(SA)k} - 1) < 0$, (7) can help j obtain a higher converged reputation for i than (5). While the node i reports a falsified sensed value, $R_{l,i}^{(SA)kt} > R_{j,i}^{(SA)kt}$ for a neighbor l that reports a spurious reputation value and so as long as $\sum_{i=0}^{s_j}(\omega_{j,i_S}^{(SA)k} - 1) < 0$, (7) can help j obtain a lower converged reputation for i than (5). Thus the first requirement for credibility is that $\sum_{i=0}^{s_j}(\omega_{j,i_S}^{(SA)k} - 1) < 0$ for a neighbor l reporting incorrectly.

In case (ii), $R_{j,i}^{(SA)kt} \approx R_{l,i}^{(SA)kt}$ for a neighbor l that also generate an spurious reputation value, then the difference between the two methods is approximately $\mu\sum_{i=0}^{s_j}(\omega_{j,i_C}^{(SA)k} - 1)(R_{l,i}^{(SA)kt} - R_{j,i}^{(SA)kt})$. While i reports incorrectly, we have $R_{l,i}^{(SA)kt} < R_{j,i}^{(SA)kt}$ for a neighbor l that reports a correct reputation value. So, as long as $\sum_{i=0}^{s_j}(\omega_{j,i_C}^{(SA)k} - 1) > 0$, (7) can help j obtain a higher converged reputation for i than (5). While i reports a correct sensed value, $R_{l,i}^{(SA)kt} < R_{j,i}^{(SA)kt}$ for a neighbor i that reports a correct reputation value and so as long as $\sum_{i=0}^{s_j}(\omega_{j,i_C}^{(SA)k} - 1) < 0$, (7) can help j obtain a lower converged reputation for i than (5). Thus the second requirement for credibility is that $\sum_{i=0}^{s_j}(\omega_{j,i_C}^{(SA)k} - 1) > 0$ for a neighbor l reporting a correct reputation value. ■

To generate the credibility $\omega_{j,i}^{(SA)k}$ that can meet the two requirements, we propose the method of:

$$\omega_{j,i}^{(SA)k} = 2 - \frac{|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}|}{\frac{\sum_{l=1}^{s_j+c_j}|R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}|}{s_j+c_j}} = 2 - \frac{(s_j+c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j}|R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} \quad (9)$$

where $\tilde{R}_{j,k}^{(SA)kt} = \frac{\sum_{l=1}^{s_j+c_j} R_{j,i}^{(SA)kt}}{s_j+c_j}$ is the average reputation value of i from neighbors of j. We have $0 \leq \omega_{j,i}^{(SA)k} \leq 2$.

The rationale for this method lies in the observation about the distances to the average reputation value. As long as there are more neighbors that report correct reputation values for i, the distance from the reputation value of a node that reports correctly to the average reputation value will be smaller than the average distance to the average reputation value, and *vice versa*. That leads to the following theorem:

Theorem. 1. *The credibility-generating method in (9) enables honest nodes to assign $\omega_{j,i}^{(SA)k} < 1$ for neighbors reporting spurious reputation, $\omega_{j,i}^{(SA)k} > 1$ for neighbors reporting correct reputation, for the reputation fusion method in (7). Therefore, (7) and (9) can help honest nodes obtain higher reputation values for other honest nodes, lower reputation values for the malicious nodes, given the condition that more neighbors report correct reputation values. This improvement of the reputation robustness can assign higher prices to the malicious nodes, lower prices to honest nodes in the spectrum allocation process.*

Proof: For a neighbor that reports spurious reputation values, the distance to the average reputation value is above average: $|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}| > \frac{\sum_{l=1}^{s_j+c_j}|R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}|}{s_j+c_j}$. Since both $s_j + c_j > 0$ and $\sum_{l=1}^{s_j+c_j}|R_{l,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)kt}| > 0$, we can have $\frac{(s_j+c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j}|R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} > 1$, which is equivalent to $2 - \frac{(s_j+c_j)|R_{j,i}^{(SA)kt} - \tilde{R}_{j,i}^{(SA)t}|}{\sum_{l=1}^{s_j+c_j}|R_{l,i}^{(SA)t} - \tilde{R}_{j,i}^{(SA)t}|} < 1$. According to (9), we have $\omega_{j,i_S}^{(SA)k} < 1$.

The proof for the case where a neighbor who reports correct reputation values is similar, and is omitted due to space constraints. Combining these two cases with the requirements on credibility, we can verify the validity of the theorem. ■

VIII. Performance Evaluation

We now present simulation results for verifying the efficacy of the proposed incentive mechanisms. In our simulations, the SNR gap β is set to 0.3. Each secondary user has the same capacity to communicate with other secondary users in its proximity. The parameters for channel gain are set as $G_{ii}^k = 1$ and $G_{ij}^k = 0.1$. The noises are $M_i^k = 10^{-11}W, \forall i \in \Omega_N, \forall k \in \Omega_K$. The transmission power of secondary users are $P_i^k = 10^{-1}W, \forall i \in \Omega_N, \forall k \in \Omega_K$. Primary users transmit with a uniform probability $\alpha_A = 0.5$ on all channels. We simulate 10 secondary users, to observe: (1) the pricing factor values generated from both sensing accuracy and sensing participation; (2) the reputation fusion process under attacks from malicious nodes.

We examine the extreme situation where malicious nodes attack on all channels, reporting falsified sensed values in the cooperative sensing process and spurious reputation values in the reputation update process. The honest but selfish secondary users participate in 10 different channels, reporting correctly sensed values in the cooperative sensing process and correct reputation values in the reputation update process.

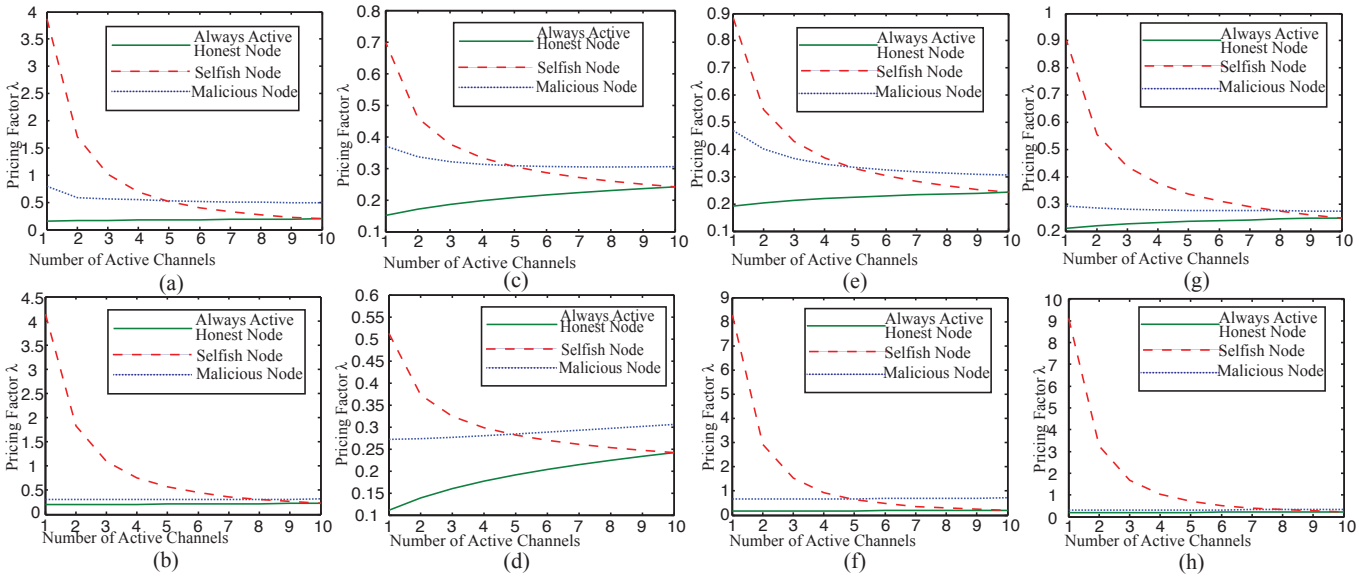

Fig. 2: Pricing Factors for an always active node, a selfish node and a malicious node. Parameters:(a) {6, 1, 3, 0.5, 0.5}. (b) {5, 1, 4, 0.5, 0.5}. (c) {4, 3, 3, 0.5, 0.5}. (d) {2, 5, 3, 0.5, 0.5}. (e) {6, 1, 3, 0.9, 0.1}. (f): {6, 1, 3, 0.1, 0.9}. (g) {5, 1, 4, 0.9, 0.1}. (h) {5, 1, 4, 0.1, 0.9}.

1) Pricing Factor: We first simulate the pricing factor for different kinds of secondary users in different situations. In Fig. 2, the x-axis indicates the number of channels a selfish node participates in, the y-axis is the pricing factor for an honest node, a malicious node or a selfish node. We use the tuple {# of always active nodes, # of selfish nodes, # of malicious nodes, ϵ, η} to denote the different parameters.

We can observe that the always active nodes have lower pricing factors compared to the malicious nodes. As the number of active channels increases, the pricing factors of the selfish nodes are eventually lowered to the same level of an always active honest node. The more active channels the selfish nodes participate in, the lower prices they can obtain. Fig. 2 (a) and (b) depict scenarios with different numbers of malicious nodes. Since malicious nodes are all actively spreading falsified sensing results on all the channels, the selfish node needs to participate in at least five channels when there are three malicious nodes, eight channels when there are four malicious nodes, to obtain a lower price than the malicious nodes. As the number of malicious nodes increases, the differences between the pricing factors of an always active honest node and a malicious node shrinks. Fig. 2 (a), (c) and (d) depict the scenarios with different numbers of selfish nodes. As the number increases, the pricing factor for a selfish node decreases. This is because the pricing factor depends on the comparable reputation values of all the nodes in the network. If other nodes have lower reputation values, the pricing factor for the selfish nodes can increase. Fig. 2 (a), (b), (e), (f), (g) and (h) depict the scenarios with different selection of parameters ϵ and η. We can observe that the higher value η is, the higher differences between the selfish node and an always active honest node. The reason is that the higher η amplifies the role of sensing participation in the pricing factor. In this case, the secondary users can be incentivized to participate on more channels. However, the importance of sensing accuracy is downplayed. This is the tradeoff between the two parameters ϵ and η. These observations indicate that the system can assign lower prices to more active honest nodes, and higher prices to malicious nodes.

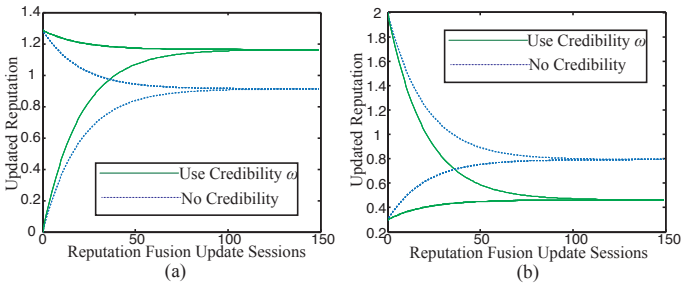

Fig. 3: Reputation Fusion Process. The reputation fusion for the $R^{(SA)}$ of (a) an honest node; (b) a malicious node.

2) Credibility: Fig. 3 depicts the differences credibility ω brings to the system performance for an honest node and a malicious node. For an honest node, the malicious nodes report the lowest reputation 0. With the help of credibility ω, the converged reputation value $R^{(SA)}$ of another honest node for the victim honest node is approximately 0.3 higher than the scenario without credibility. For a malicious node, the other malicious nodes report extremely high reputation values 2. With the help of credibility ω, the converged reputation value $R^{(SA)}$ of an honest node for the malicious node is approximately 0.4 lower than the scenario without credibility. These observations indicate that the system can improve the robustness of reputation by reducing the effect of spurious reputation values.

IX. Conclusion

We propose to use reputation as a pricing factor in the spectrum allocation process to incentivize cooperative sensing in distributed CRNs. The reputation values are generated from both sensing accuracy and sensing participation. Both theoretical analysis and simulation results indicate that this method can incentivize secondary users to participate in more channels and report more accurate sensing reports, in order to obtain lower prices in the spectrum allocation process. To countermeasure attacks in the reputation fusion process where malicious nodes report spurious reputation values, we proposed a method with the help of other honest neighbors. Our methods, from cooperative spectrum sensing to reputation fusion then to spectrum allocation, are entirely distributed without a central authority, and thus more applicable to distributed CRNs.

Appendix

The calculation of the optimal pricing factor as shown in (3) is:

$$\begin{aligned}
\lambda_i^k &= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\partial u_j(P_j^k)}{\partial P_i^k}}{R_i} \\
&= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\partial[\alpha_A \log_2(1+\frac{\beta G_{jj}^k P_j^k}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k})]}{\partial P_i^k}}{R_i} \\
&= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\partial[\alpha_A \log_2(1+\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k})]}{\partial P_i^k}}{R_i} \\
&= -\frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha_A}{\ln 2} \frac{\frac{\partial(\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k})}{\partial P_i^k}}{1+\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k}}}{R_i} \\
&= \frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha_A}{\ln 2} \frac{\frac{G_{ij}^k \beta G_{jj}^k P_j^k}{(G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k)^2}}{1+\frac{\beta G_{jj}^k P_j^k}{G_{ij}^k P_i^k + \sum_{l\in\Omega_N, l\neq j, i\neq j} G_{ij}^k P_i^k + M_j^k}}}{R_i} \\
&= \frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha_A}{\ln 2} \frac{\frac{G_{ij}^k \beta G_{jj}^k P_j^k}{(\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k)^2}}{1+\frac{\beta G_{jj}^k P_j^k}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k}}}{R_i} \\
&= \frac{\sum_{j\in\Omega_N, j\neq i} R_j \frac{\alpha_A}{\ln 2} \frac{\frac{G_{ij}^k \beta G_{jj}^k P_j^k}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k + \beta G_{jj}^k P_j^k}}{\sum_{i\in\Omega_N, i\neq j} G_{ij}^k P_i^k + M_j^k}}{R_i},
\end{aligned}$$

which can be easily transformed to the final result of λ_i^k.

References

[1] V. Krishnamurthy, M. Maskery, and G. Yin, Decentralized Adaptive Filtering Algorithms for Sensor Activation in An Unattended Ground Sensor Network, *IEEE Transactions on Signal Processing*, vol. 56, no. 12, pp. 6086-6101, Dec. 2008.

[2] A. Mukherjee, Diffusion of Cooperative Behavior in Decentralized Cognitive Radio Networks with Selfish Spectrum Sensors, *IEEE Journal of Selected Topics in Signal Processing*, vol. 7, no. 2, pp. 175-183, April 2013.

[3] T. Jiang, H. Wang, and A. Athanasios, QoE-Driven Channel Allocation Schemes for Multimedia Transmission of Priority-Based Secondary Users over Cognitive Radio Networks, *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 7, pp. 1215-1224, Aug. 2012.

[4] R. Xie, F. R. Yu, and H. Ji, Dynamic Resource Allocation for Heterogeneous Services in Cognitive Radio Networks with Imperfect Channel Sensing. *IEEE Transactions on Vehicular Technology*, vol. 61, no. 2, pp. 770-780, Feb. 2012.

[5] R. Xie, F. R. Yu, H. Ji, and Y. Li, Energy-Efficient Resource Allocation for Heterogeneous Cognitive Radio Networks with Femtocells. *IEEE Transactions on Wireless Communications*, vol. 11, no. 11, pp. 3910-3920, Nov. 2012.

[6] Q. Liang, S. Han, F. Yang, G. Sun, and X. Wang, A Distributed-Centralized Scheme for Short- and Long- Term Spectrum Sharing with a Random Leader in Cognitive Radio Networks, *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2274-2284, Dec. 2012.

[7] L. T. Tan, and L. B. Le, Channel Assignment with Access Contention Resolution for Cognitive Radio Networks, *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2808-2823, July 2012.

[8] S. Wang, Z, -H. Zhou, M. Ge, and C. Wang, Resource Allocation for Heterogeneous Cognitive Radio Networks with Imperfect Spectrum Sensing, *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 3, pp. 464-475, March 2013.

[9] Y. Tachwali, B. F. Lo, I. F. Akyildiz, and R. Augustí, Multiuser Resource Allocation Optimization Using Bandwidth-Power Product in Cognitive Radio Networks, *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 3, pp. 451-463, March 2013.

[10] F. Wang, M, Krunz, and S. Cui, Price-Based Spectrum Management in Cognitive Radio Networks, *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 74-87, Feb. 2008.

[11] H, -P, Shiang, and M. van der Schaar, Distributed Resource Management in Multi-hop Cognitive Radio Networks for Delay Sensitive Transmission, *IEEE Transactions on Vehicular Technology*, vol. 58, no. 2, pp. 941-953, Feb. 2009.

[12] L. Cao, and H. Zheng, Distributed Rule-Regulated Spectrum Sharing, *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 130-145, Jan. 2008.

[13] T. Zhang, R. Safavi-Naini, and Z. Li, ReDiSen: Reputation-based Secure Cooperative Sensing in Distributed Cognitive Radio Networks, *Proceedings of the 2013 IEEE International Conference on Communications (ICC)*, pp. 1194-1198, June 2013.

[14] Z. Li, F. R. Yu, and M. Huang, A Distributed Consensus-Based Cooperative Spectrum-Sensing Scheme in Cognitive Radios, *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 383-393, Jan. 2010.

[15] C. Song, and Q. Zhang, Achieving Cooperative Spectrum Sensing in Wireless Cognitive Radio Networks, *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 14-25, April 2009.

[16] B. Wang, K. Liu, and T. Clancy, Evolutionary Cooperative Spectrum Sensing Game: How to Collaborate? *IEEE Transactions on Communications*, vol. 58, no. 3, pp. 890-900, March 2010.

[17] S. Li, H. Zhu, Z. Gao, X. Guan, and K. Xing, YouSense: Mitigating Entropy Selfishness in Distributed Collaborative Spectrum Sensing, *Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM 2013)*, pp. 2635-2643, April 2013.

[18] R. Olfati-Saber, J. A. Fax, and R. M. Murray, Consensus and Cooperation in Networked Multi-Agent Systems, *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215-233, Jan. 2007.

[19] I. F. Akyildiz, B. F. Lo, and R.Balakrishnan, Cooperative spectrum sensing in cognitive radio networks: A survey, *Physical Communication* vol. 4, no. 1, pp. 40-62, March 2011.

[20] J. W. Mwangoka, K. B. Letaief, and Z. Cao, Joint Power Control and Specturm Allocation for Cognitive Radio Networks via Pricing, *Physical Communication* vol. 2, no. 1-2, pp.103-115, March - June 2009.

[21] I. Atzeni, L. G. Ordóñez, G. Scutari, D. P. Palomar, and J. R. Fonollosa, Noncooperative and Cooperative Optimization of Distributed Energy Generation and Storage in the Demand-Side of the Smart Grid, *IEEE Transactions on Signal Processing*, vol. 61, no. 110, pp. 2454-2472, May 2013.

[22] D. A. Schmidt, C. Shi, R. A. Berry, M. L. Honig, and W. Utschick, Distributed Resource Allocation Schemes, *IEEE Signal Processing Magazine*, vol. 26, no. 5, pp.53-63, Sept. 2009.

[23] A. A. El-Sherif, and K. J. R. Liu, Joint Design of Spectrum Sensing and Channel Access in Cognitive Radio Networks, *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp.1743-1753, June 2011.