Coalition based Optimization of Resource Allocation with Malicious User Detection in Cognitive Radio Networks

Xiaoge Huang[1], Liping Chen[1], Qianbin Chen[1] and Bin Shen[1]
[1]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongwen Road, 400065 Chongqing, China
[Email: Huangxg@cqupt.edu.cn]
*Corresponding author: Xiaoge Huang

Received February 8, 2016; revised June 4, 2016; accepted July 22, 2016; published October 31, 2016

Abstract

Cognitive radio (CR) technology is an effective solution to the spectrum scarcity issue. Collaborative spectrum sensing is known as a promising technique to improve the performance of spectrum sensing in cognitive radio networks (CRNs). However, collaborative spectrum sensing is vulnerable to spectrum data falsification (SSDF) attack, where malicious users (MUs) may send false sensing data to mislead other secondary users (SUs) to make an incorrect decision about primary user (PUs) activity, which is one of the key adversaries to the performance of CRNs. In this paper, we propose a coalition based malicious users detection (CMD) algorithm to detect the malicious user in CRNs. The proposed CMD algorithm can efficiently detect MUs base on the Geary'C theory and be modeled as a coalition formation game. Specifically, SSDF attack is one of the key issues to affect the resource allocation process. Focusing on the security issues, in this paper, we analyze the power allocation problem with MUs, and propose MUs detection based power allocation (MPA) algorithm. The MPA algorithm is divided into two steps: the MUs detection step and the optimal power allocation step. Firstly, in the MUs detection step, by the CMD algorithm we can obtain the MUs detection probability and the energy consumption of MUs detection. Secondly, in the optimal power allocation step, we use the Lagrange dual decomposition method to obtain the optimal transmission power of each SU and achieve the maximum utility of the whole CRN. Numerical simulation results show that the proposed CMD and MPA scheme can achieve a considerable performance improvement in MUs detection and power allocation.

Keywords: Cognitive radio network, malicious user detection, coalition formation game, power allocation

This work is supported by the National Natural Science Foundation of China (NSFC) (61401053, 61201205), the 863 project No.2014AA01A701, Changjiang Scholars and Innovative Research Team in University (IRT1299), Special Fund of Chongqing Key Laboratory (CSTC)

http://dx.doi.org/10.3837/tiis.2016.10.003 **ISSN : 1976-7277**

1. Introduction

The increasing of wireless services is accompanied with a huge demand on the spectrum resource. However, most of the channels have already been allocated according to static spectrum allocation policy. Various reports have shown that the licensed spectrum remains unoccupied for more than 70% periods [1]. The concept of cognitive radio (CR) has been considered as a promising technology to improve spectrum utilization.

CR technology allows the secondary users (SUs) to employ the spectrum holes by licensed primary users (PUs) with limited the performance degradation caused to PUs' communication, which can improve spectrum utilization and enhance the efficiency of spectrum sharing [2]. For the initial step, SUs sense the licensed spectrum and collect the information of PUs for available opportunities, which is the basis for all implementations. Thus the design of reliable and accurate spectrum sensing method is crucial to CR technology. However, the sensing performance is susceptible to the fast changing wireless environment and interference signal due to the openness of spectrum and non-protective and competitiveness of SUs' opportunistic access [3]. Moreover, owing to the openness of wireless channels and the selfish behavior of SUs, CR networks are suffered from various kinds of security issues or attacks such as spoofing, jamming, and wiretap, etc [4]. Spectrum sensing attack is one of the security issues and it can be grouped into two major categories: primary users emulation (PUE) attack, the attacker emulates the characteristics of the PU to obtain exclusive spectrum usage [5]; spectrum sensing data falsification (SSDF) attack, attackers may report incorrect sensing data to neighboring SUs or fusion center (FC) leading to a degradation on performance of the collaborative spectrum sensing [6]. In this paper, we focus on the SSDF attack and call the attackers as malicious users (MUs).

1.1 Related Work

The novel analysis on attacks and defense strategies attract people's attention in recent years for new security threats and challenges in CR network (CRN). Notably, as the focus of this paper, the research on SSDF attack and defense has gained significant achievements recently [7]-[13]. The approaches of SSDF attacks detection depend on the types of MUs as well as spectrum sensing results from SUs. In [7], the authors proposed a scheme to detect SSDF attack by dynamic learning the behavior of SUs in cooperative spectrum sensing (CCS) but they did not analyze the consociation of attackers. In [8], a reputation-based CCS with the assistance of honest users is proposed. However, the proposed scheme cannot be applied to the scenario that sensing results of all SUs are far from those of honest users, and leads little contribution to final decision. In [9], the authors proposed a defense scheme using kernel-based learning methods and statistical signal processing method in combination, which focus on statistical analysis of the sensing signal of SUs at the price of energy consumption. In [10], the authors propsed a muti-channels based detection technique by comparing the sensing reports of neighboring SUs, which can be applied in the scenario with 20% MUs. According to [11], Min et al. considered to use the shadow fading correlation to detect MUs, which can reduce the impact of MUs on the performance of distributed cooperative sensing. A detection scheme proposed in [12] utilizes the outlier of energy sensors, considering a centralized spectrum sensing and a few MUs. In addition, a detection scheme proposed in [13] utilizes the spatial information correlation between SUs, which can be just applied in the scenario with a few MUs at the cost of much energy consumption. Above mentioned detection schemes are

suitable for a few MUs and do not consider energy consumption in the process of MUs detection.

SUs decided to access the idle channels belong to the PUs based on the sensing results, and optimize the power allocation to achieve a higher efficiency of the spectrum resource while limiting the performance degradation cause to PUs. Specifically, the effects of SSDF attack on the resource allocation process reflect in two aspects: 1) the false sensing results of malicious users mislead the detection of primary users and influence the spectrum access of other secondary users; 2) malicious users would send false information to decrease the communication quality of other SUs. The traditional resource allocation problem in CRNs has been widely studied in the literature [14]-[17]. In [14], the authors proposed a centralized optimal power allocation to the cognitive transmitters, which considers the maximum interference constraint of PUs and minimum SINR constraint of SUs. The performance of power allocation in cooperative approaches is better than the non-cooperative ones according to [15], in which the authors proposed a optimization algorithm to maximize the utility in multi-cell CRNs, involving the exchange of prices to deal with the interference between cells and using cooperative power allocation approaches to improve the total sum-rate. A sensing-based power allocation model is proposed in [16], where the influence from the sensing probability is considered and the total throughput over multi-variables is optimized. Furthermore, joint cell selection and power allocation problem are analyzed in CR small cell network in [17].

Focusing on the security issues, a novel analysis is proposed in this paper, which combines MUs detection with the impact on optimal power allocation in CRNs. The traditional MUs detection schemes don't work well with the SSDF attack, in order to improve the MU detection accuracy, the spatial correlation theory is used to detect independent and cooperative attack from MUs. In addition, the MUs detection process is performed as a coalition formation game which is able to achieve the highest accuracy of MUs detection. Specifically, the energy consumption in the MUs detection process as well as the degree of participation is considered in the optimization problem.

1.2 Contribution

In the paper, we analyze the resource allocation problem among CRNs based on malicious users detection scheme, where the MUs detection process is considered as a coalition game, and the Geary'C theory is used to improve the MUs detection accuracy. The main contributions of this paper can be summarized as follows:

- Coalition based Malicious users Detection: We design a coalition based MUs detection algorithm for CRNs. The Geary'C theory [18] is the core of MUs detection, which is used to calculate the spatial correlation of SUs between their neighbors. According to the difference of spatial correlation between honest users (HUs) which report true sensing result and malicious users (MUs) which launch the SSDF attack, the MUs could be detected. The CMD algorithm can be applied to both independent and collaborative attack of MUs, which can achieve considerable performance improvement compared with the traditional MUs detection method.
- Coalition Game Modeling of MUs Detection: The process of MUs detection algorithm can be formulated as a coalition formation game with a nontransferable utility to effectively improve the probability of MUs detection while decrease energy consumption. In the coalition game, the players are all the SUs in CRNs, and the utility function is composed of the accuracy of MUs detection and energy consumption factors of each

coalition. SUs adjust the coalition partition base on the Pareto order and record the partition to guarantee the stability of the game.

- MUs Detection based Power Allocation Algorithm: The optimal power allocation problem jointly considering the impact from MUs with untruthful or false behavior. The problem is a multi-variable optimization problem which consists of three parts: sum-rate of SUs, the detection probability of MUs and energy consumption by MUs detection. According to its convex characteristic, dual decomposition is used in this paper to solve the problem.

The rest of the paper is organized as follows. In Section 2, we describe the topology of system model. The coalition based MUs detection algorithm and the associate a coalition game are presented in Section 3. In Section 4, we analyze the MUs detection based optimal power allocation algorithm which can be solve by the dual decomposition method. The simulation results are presented and discussed in Section 5 and finally the conclusions are drawn in Section 6.

2. System Model

In this section, we present the topology of CRNs and analyze both independent and collaborative SSDF attack models.

2.1 Network Model

We consider a CRN comprised of one PU, one SU base station (SBS) acts as the FC of N SUs, where a half-duplex stationary transmission model is used. The number of channels available for SU i (i.e. PU is absent in this channel temporarily) is M. Note that a channel can only be assigned to one SU. According to the behavior of SUs, they are divided into two types: HUs and MUs. Namely, HUs: SUs sense the PU channel and report the faithful sensing results to the FC; MUs: SUs would tamper the sensing data based on their intention before sending to the FC, which leads to a wrong decision by FC about the actual status of PUs and degrade the CRN performance. Moreover, once MUs access the idle channels, they could attempt to prohibit HUs from using the channels which decrease the probability of HUs to use the idle channel. We focus on the number of MUs is less than HUs since it is meaningless to study a network where a majority of users are malicious. The system model is shown in **Fig. 1**.

Energy detectors is used to detect the presence of the PU, the probability of detection and false alarm of SU i are given by $P_{d,i}$and $P_{fa,i}$ respectively [19]:

$$P_{d,i} = P\{Y > \lambda | H_1\} = Q((\lambda - \gamma_i)\sqrt{\tau_s f_s/(2\gamma_i - 1)}) \quad (1)$$

$$P_{fa,i} = P\{Y > \lambda | H_0\} = Q((\lambda - 1)\sqrt{\tau_s f_s}) \quad (2)$$

where hypothesis H_0 represents the absence of PU while H_1 states the present. Y denotes the obtained statistic energy from the PU, λ is the decision threshold of the energy detector, γ_i is the received SNR of SU i from the PU, f_s represents the sampling frequency and τ_s means the sensing time. The noise at the SUs is assumed to be independent and identically distributed Gaussian noise $\mathcal{N}(0,1)$. The received power of SU i from the PU can be expressed as [20]:

$$P_i^r = P_t - (10\mu_o \lg(d_i/d_o)) + G_i)(dB) \quad (3)$$

where P_t is the transmit power of the PU, μ_o is the path-loss exponent, d_i is the distance from the PU to SU i, and d_o is the reference distance, G_i is the log-normal shadowing coefficient which can be accounted by e_i^X where $X_i \backsim \mathcal{N}(0, \sigma^2)$.

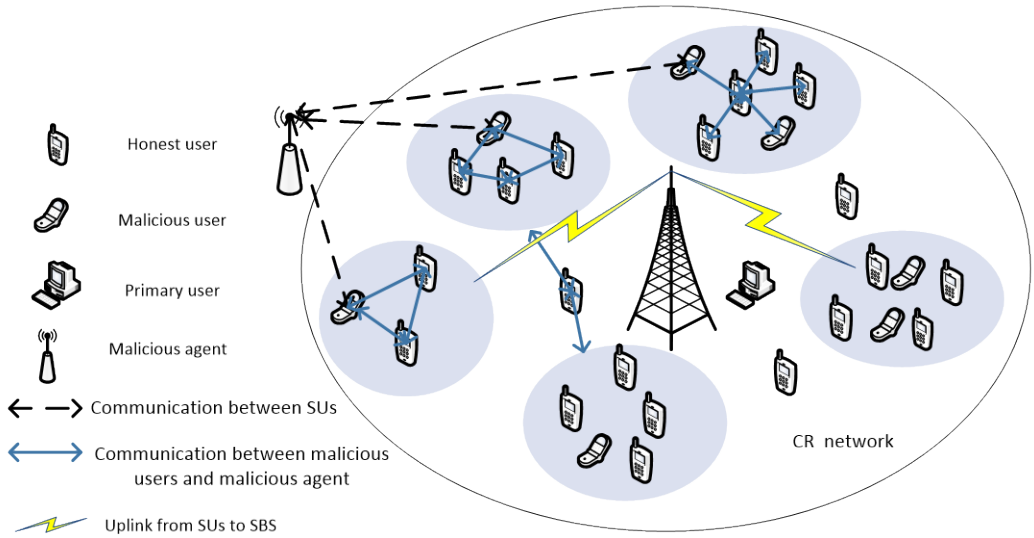

Fig. 1. System model

2.2 Attack Model

We consider two kinds of attacking strategies: independent attack and collaborative attack [21]. For independent attack, MUs report false sensing results based on their own profit, MUs may report a lower detection probability of the PU for disturbing the normal operation of PU systems, or report a higher false alarm probability in order to decrease access opportunities of HUs.

For collaborative attack, a malicious agent (MA) is located on the edge of the CRN, which is the control consoler of MUs. Firstly, MUs send faithful sensing results to the MA. The MA makes the decision based on sensing results from MUs. Then the MA adjusts the detection decisions to launch the cooperative attack before sending them back to MUs. Finally, all MUs report the received decisions from MA to the FC.

3. Coalition based Malicious Users Detection Algorithm

The MUs could cause serious security threats in CRNs, through falsifying their sensing output and increasing false alarms. MUs could obtain more opportunities at the cost of HUs' loss, which decreases the sum-rate of the whole CRN while increasing the interference to the PU system. In order to detect MUs efficiently we provide a coalition based MUs detection scheme, which could detect the MUs by a cooperative manner and achieve much higher detection accuracy than the methods in the literatures.

3.1 Coalition Formation

Based on local sensing results from Eq. (1), SU i needs to search potential cooperative SUs, namely, its neighbors under the following conditions:

- Step1: If SU j satisfies $\left|P_{d,i} - P_{d,j}\right| \leq$ a, the SU j is considered as one of SU i's neighbors and enter into the same coalition, where $P_{d,i}$ and $P_{d,j}$ are the sensing results of SU i and SU j respectively.

- Step2: If SU i is selected to join the coalition partition, other SUs with the maximum $P_{d,i}$ would be selected from the remaining sets $\boldsymbol{N}_{\mathrm{R}} = \{\boldsymbol{N} - i\}$, and repeat Step1.
- Step3: After Step1 and Step2, the remaining disjoint SUs chose join the nearest coalition until no single SU exist.
- Step4: Adjust the coalition partition base on the merge and split order until find the optimal coalition partition $\mathcal{T}_{\mathrm{n}}^{*} = \arg\ \max_{\mathcal{T}_{\mathrm{n}\in\mathrm{T}}} \mathrm{V}(\mathcal{T}_{\mathrm{n}})$.

3.2 Geary'C Theory

Due to the selfish behavior, MUs may decrease the performance of cooperative sensing of the whole CRN to obtain more profit. In order to distinguish MUs in each coalition depend on their behaviors, we use the Geary'C theory. Geary'C theory is one of the spatial statistics indicators to determine if adjacent observations of the same phenomenon are correlated, which is useful to find the difference partly measures the autocorrelation between a user and its neighboring users. The Geary'C can be expressed as follows [18]:

$$C = \frac{\tilde{n}-1}{\sum_{i=1}^{\tilde{n}} w_{ij}(y_i-\bar{y})^2} \frac{\sum_{i=1}^{\tilde{n}}\sum_{j=1}^{\tilde{n}} w_{ij}(y_i-y_j)^2}{2\sum_{i=1}^{\tilde{n}}\sum_{j=1}^{\tilde{n}} w_{ij}} \tag{4}$$

where $\tilde{n}$ is the number of all units in local range, y_i and y_j are pixel value of unit i and unit j. $\bar{y}$ is the mean of pixel value of all units, w_{ij} is the weight factor between unit i and unit j. The Geary'C theory presents the correlations between all units.

In our system model, SUs are regarded as units whereas a coalition is considered as the local range. The pixel value of a unit is regarded as the received power of SUs from PU. In fading environment, sensing results from nearby HUs are similar. Therefore, based on the Geary'C theory, HUs have smaller spatial correlation compared with MUs in a coalition. Each SU takes turns as the coalition head to make the final decision for a coalition. Assume MUs cannot adjust the sensing report collected from others, thus the coalition head can make a true decision. We use Geary'C theory to calculate the spatial correlation of SU $i \in S_k$ which is the autocorrelation between SU i and its neighboring SUs in coalition S_k is denoted as $C_i(S_k)$:

$$C_i(S_k) = \frac{\sum_{j=1}^{n_k} w_{ij}(P_i^r - P_j^r)^2}{\frac{1}{n_k-1}\sum_{j=1}^{n_k} w_{ij}(P_i^r - \overline{P^r})^2} \tag{5}$$

where n_k is the number of SUs in S_k, P_i^r and P_j^r are received power of SU i and SU j from PU, $\overline{P^r}$ is the average received power of SUs in coalition S_k. $w_{ij} = d_{ij}^{-1}$ is the weight factor of spatial correlation between SU i and SU j, and d_{ij} is the distance between SU i and SU j.

Notably, the values of $C_i(S_k)$ lie between 0 and the given thresholds ε_0, ε_1 and ε_2. Values of $C_i(S_k)$ lie in the proper range mean the correlation between SU i and other SUs in S_k is positive, which show that SU i is a HU, otherwise, it is a MU.

Furthermore, the percentage of MUs in coalition S_k also could affect the value of $C_i(S_k)$. Notably, even we focus on the case when the total percentage of MUs is less than 50%, the tough case when the percentage of MUs is more than 50% could happen. We consider two kinds of scenario with respect to the percentage of MUs in each coalition, that are, Honest Case and Suspected Case:

- Honest Case (HC): the percentage of MUs is less than 50% of S_k.

$$D_i(S_k) = \begin{cases} 1 & \text{if } C_i(S_k) > \varepsilon_0 \\ 0 & \text{if } C_i(S_k) \le \varepsilon_0 \end{cases} \tag{6}$$

- Suspected Case (SC): the percentage of MUs is more than 50% of S_k.

$$D_i(S_k) = \begin{cases} 1 & \text{if } \varepsilon_1 < C_i(S_k) < \varepsilon_2 \\ 0 & \text{if } C_i(S_k) \ge \varepsilon_2 \ \text{ or } C_i(S_k) \le \varepsilon_1 \end{cases} \tag{7}$$

where $D_i(S_k) = 1$ denotes that SU *i* is considered as a MU, otherwise $D_i(S_k) = 0$. ε_0, ε_1 and ε_2 are given decision thresholds. $\overline{P^r}$ is critical for calculating the spatial correlations of SUs in S_k. In HC, $\overline{P^r}$ is the dominate factor for spatial correlation of SUs and the difference between the spatial correlations of HUs and MUs is clear. However, in SC, there are more MUs than HUs, which increases the difficulty of MUs detection. Since the distinction of the spatial correlations between HUs and MUs are tiny. To overcome this problem, double threshold ε_1 and ε_2 are used here to enhance the detection accuracy. The optimal values of threshold ε_0, ε_1 , ε_2 can be obtained by exhausted search method.

The detection probability of MUs $P_d^M(S_k)$ and energy consumption of detecting MUs $E_i^D(S_k)$ in are two important factors which should be taken into consideration during in coalition formation. $P_d^M(S_k)$ can be formulated as: $P_d^M(S_k) = n_k^d/n_k$, where n_k is the number of SUs in S_k and n_k^d is the number of MUs in S_k which can be correctly detected.

3.3 Energy Consumption

The total energy consumption of SU *i* $E_i^T(S_k)$ in S_k can be divided into two parts: energy consumption for MUs detection $E_i^D(S_k)$ and energy consumption for information transmission to SBS in uplink $E_i^U(S_k)$. $E_i^D(S_k)$ is related to the communication between SU *i* and other SUs in S_k which consist of two parts:

- Calculate spatial correlation: SU *i* report the sensing results of PU to the head of S_k and the head of S_k calculate spatial correlation in S_k.
- Make decision: SU *i* take turns to performed as the head of S_k to make decision and broadcast the detection result to all the SUs in S_k.

Meanwhile, $E_i^U(S_k)$ comes from five parts [22]:

- Transceiver Chain $E_i^{TC}(S_k)$: the energy consumption of typical transmitters and receivers for SU *i*.
- Channel Estimation $E_i^{CE}(S_k)$: the energy consumption of the uplink channel estimation process from SU *i* to the SBS.
- Coding and Decoding $E_i^{CD}(S_k)$: SU *i* applies channel coding and modulation to information symbols in the uplink.
- Linear Processing $E_i^{LP}(S_k)$: The transmitted and received vectors of information symbols at the SBS are generated by transmit precoding and processed by receive combining.

In general, the total energy consumption of SU *i* in coalition S_k is given as follows:

$$E_i^T(S_k) = E_i^D(S_k) + E_i^U(S_k) = E_i^D(S_k) + E_i^{TC}(S_k) + E_i^{CE}(S_k) + E_i^{CD}(S_k) + E_i^{LP}(S_k) \quad (8)$$

3.4 Coalition Formation Game

Depending on the sensing results and the spatial correlation of SUs, the SUs could decide their coalitions to detect the MUs. The structure of coalition formation directly affects the accuracy and the energy consumption of MUs detection in a coalition. To devise suitable cooperative strategies among the SUs, we model the coalition formation as a coalitional game with a non-transferable utility which provides useful tools to decide the optimal coalition partition. To model the game, we make the following definitions:

Coalition Formation Game: Let $\mathrm{G} = \{\mathcal{N}, \mathrm{v}\}$ be a coalition game with a non-transferable utility [23], where $\mathcal{N}$ is the set of players SU $i \in \mathcal{N}$, and v is utility function of the game.

Coalition Partition: A coalition partition is a distribution of players $\mathcal{N}$ forming disjoint coalitions in CRN. The set of all possible coalition partitions is denoted as $T = \{\mathcal{T}_0, \mathcal{T}_1, \dots, \mathcal{T}_n\}$,

where $\mathcal{T}_n$ represents the coalition partition of the CRN at iteration n. We define the initial state $\mathcal{T}_0 = \{\{1\}, \dots, \{N\}\}$ which composed of singletons of player.

Utility: A non-transferable utility $v(S_k, \mathcal{T}_n)$ of coalition S_k at iteration n is denoted as the objective function, which is given as:

$$v(S_k, \mathcal{T}_n) = \begin{cases} P_d^M(S_k) - \frac{\sum_{i=1}^{n_k} E_i^D(S_k)}{E_{max}} & \text{if } 0 \le n \le n_m \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

where $P_d^M(S_k)$ is the detection probability of MUs and $E_i^D(S_k)$ is energy consumption of detecting MUs of SU i in S_k. $E_{max} = l_o d_{max}^2$ is the maximum energy consumption of SU i, where d_{max} is maximum distance between arbitrary two SUs and l_o is the energy consumption per kilometer. n_m is the maximum number of SUs per coalition can be served. It is clear that energy consumption increase with the increasing number of SUs per coalitions while the probability of detection and false alarm for PU will increase simultaneously. Notably, $v(S_k, \mathcal{T}_n)$ is not divisible among the SUs since the utility of SU i in S_k is equal to $v(S_k, \mathcal{T}_n)$, namely, satisfy $v_i(S_k, \mathcal{T}_n) = v(S_k, \mathcal{T}_n)\ \forall\, i \in S_k$, where $v_i(S_k, \mathcal{T}_n)$ is the utility of SU i in coalition S_k for the non-transferable utility of coalition formation game [24].

Thus, the total utility $V(\mathcal{T}_n)$ of the CRN at iteration time n is given by:

$$V(\mathcal{T}_n) = \sum_{j=1}^{|\mathcal{T}_n|} v(S_k, \mathcal{T}_n) \tag{10}$$

where $|\mathcal{T}_n|$ is the number of coalition at iteration n.

According to [23], we apply Pareto order to adjust the structure of coalitions based on twofold: firstly, increase $P_d^M(S_k)$ which could enhance the performance of CRNs while decrease disturbing the normal operation of PU systems; and secondly, decrease $E_i^D(S_k)$ with the purpose of maximizing the total utility of the CRN.

Coalition Repartition: At iteration n, SU i choose to deviate from one coalition to another only if the following conditions are satisfied:

$$\begin{cases} V(\mathcal{T}_{n+1}) > V(\mathcal{T}_n) \\ v(\tilde{S}_k, \mathcal{T}_{n+1}) > v(S_k, \mathcal{T}_n) \end{cases} \tag{11}$$

where $\tilde{S}_k$ is the new coalition, if SU i joins S_k at iteration n, $\tilde{S}_k = S_k \cup \{i\}$, and the coalition partition turns from $\mathcal{T}_n$ to $\mathcal{T}_{n+1}$. $V(\mathcal{T}_n)$ is the total utility of CRNs at iteration n.

For two coalition S_k and S_{-k}, where S_{-k} denotes one of the coalitions except S_k, they choose to merge as a new coalition only if the following condition are satisfied:

$$\begin{cases} V(\mathcal{T}_{n+1}) > V(\mathcal{T}_n) \\ v(\tilde{S}_k, \mathcal{T}_{n+1}) > v(S_k, \mathcal{T}_n) + v(S_{-k}, \mathcal{T}_n) \end{cases} \tag{12}$$

where $\tilde{S}_k$ is the new coalition, e.g. S_k decides to merge to S_{-k} at iteration n, S_k and S_{-k} merge, $\tilde{S}_k = \{S_k \cup S_{-k}\}$. The coalition partition $\mathcal{T}_n$ will be recorded to avoid the coalition game getting into infinite loops and guarantee the coalition game can achieve the equilibrium.

Coalition Partition Record: Denote $\mathcal{H} = \{h_0, h_1, \dots, h_n\}$ as the record set at iteration n, where $h_n = \left(V(\mathcal{T}_n), \{v(S_1, \mathcal{T}_n), \dots, v(S_k, \mathcal{T}_n), \dots, v(S_{|\mathcal{T}_n|}, \mathcal{T}_n)\}\right)$ presents the total utility of CRN and individual utility of each coalition at iteration n. The record set $\mathcal{H}$ guarantees that the same coalition partition cannot be appeared in the coalition formation process. If $\mathcal{T}_{n+1} \neq \mathcal{T}_n$, h_{n+1} is not equal to any records in $\mathcal{H}$, $\mathcal{H} = \{h_0, h_1, \dots, h_n, h_{n+1}\}$ at iteration n+1 otherwise the coalition optimization reaches convergence.

Specifically, if one of the following conditions is satisfied, coalition repartition stops: 1) If the record set $\mathcal{H}$ includes all the possible records and all the possible coalition partition of the CRN; 2) If the coalition partition achieves the optimal, the utility of the CRN based on the energy consumption and the MU detection probability achieves the maximum. To

demonstrate the stability of the proposed coalition game, we introduce the conception of defection function D, D_{hp}, D-stable and D_{hp}-stable as following [25]:

Definition 1 A defection function D is the function that can map each partition $\mathcal{T}_n$ of $\mathcal{N}$ into a group of collections in $\mathcal{N}$. A partition is D-stable if no players intend to leave $\mathcal{T}_n$ to form the collections allowed by D.

Specifically, if the partition $\mathcal{T}_n$ is D-stable, the partition is Pareto optimal. However, the partition is not ever-present. The D-stable exits only with the following two conditions [23]:

- For each pair of disjoint sub-coalitions S_1^S and S_2^S in $S_k \in \mathcal{T}_n$, $v\left(S_1^S \cup S_2^S\right) > v(S_2^S)$ or $v\left(S_1^S \cup S_2^S\right) > v(S_1^S)$ is satisfied.
- For the partition $\mathcal{T}_n = \{S_1, \dots, S_{|\mathcal{T}_n|}\}$, a incompatible coalition $S' \in \mathcal{N}$ formed by SUs belonging to different $S_k \in \mathcal{T}_n$. If the partition $\mathcal{T}_n$ is D-stable, all incompatible coalitions should satisfy $v(S' \cap S_k) > v(S')$, $\forall k \in \{1, \dots, |\mathcal{T}_n|\}$.

Definition 2 A defection function D_{hp} is the function that can map a partition $\mathcal{T}_n$ of $\mathcal{N}$ into a partition based on merge-split operation. A partition $\mathcal{T}_n = \{S_1, \dots, S_{|\mathcal{T}_n|}\}$ is D_{hp}-stable if no group of players could leave only using merge-split operation and form new partitions.

We use Pareto order as the comparison relation which is monotonous, transitive and linear and rule is merge-split.

***Lemma* 1** For an arbitrary coalition formation game, the comparison relation is monotonous, transitive, irreflexive and linear, and it can reach the optimal D-stable partition if such a partition exists. Otherwise, the final network partition is D_{hp}-stable [25].

In this paper, the coalition formation game reaches stable, only if there are no SUs change their coalitions, and the utility of the whole CRN $V(\mathcal{T}_n^*)$ achieve the maximum where the coalition partition $\mathcal{T}_n^*$ is called the optimal coalition partition.

The process of coalition formation game is summarized as follows:

- Coalition Formation: SUs search potential coalition members by broadcast their local sensing results, which cause two kinds of forms. Split: SU i leaves S_k and joins S_{-k}; Merge: S_k merge to S_{-k} and form $\tilde{S}_k$.
- Coalition Partition: Calculate the total utility of the CRN $V(\mathcal{T}_{n+1})$ and utility of each coalition in potential partition $v(S_k, \mathcal{T}_{n+1})$. Compare the utility between current coalition partition $\mathcal{T}_n$ and potential coalition partition $\mathcal{T}_{n+1}$ to decide whether to set the coalition repartition.
- Coalition Partition Record Update: If $\mathcal{T}_n$ turns $\mathcal{T}_{n+1}$ the new record $h_n = \left(V(\mathcal{T}_{n+1}), \left\{v(S_1, \mathcal{T}_{n+1}), \dots, v(S_k, \mathcal{T}_{n+1}), \dots, v\left(S_{|\mathcal{T}_{n+1}|}, \mathcal{T}_{n+1}\right)\right\}\right)$ are stored in the record $\mathcal{H}$. Otherwise, the record set $\mathcal{H}$ remains unchanged.
- Coalition Stabilize: Repeat above three steps until reach the convergence of the coalition partition.

The four steps of the coalition formation are repeated till no SUs intent to leave the current partition, resulting in a stability partition.

Proof : The proof for the stability of the proposed coalition game is given in Appendix A.

We outline the coalition based malicious user detection (CMD) algorithm in **Table 1**.

Table 1. Coalition based Malicious User Detection (CMD) Algorithm

Coalition based Malicious User Detection (CMD) Algorithm
1. Initialization:
MUs and SUs are randomly distributed in the given range, initialize the coalition $\mathcal{T}_0 = \{\{1\}, \dots, \{N\}\}$ and the record set $\mathcal{H} = \{h_0\}$, n=0.
2. Local Spectrum Sensing:

SUs obtain the sensing results of PUs by Eq.(1) and Eq.(2)
3. **Step 1: Coalition Partition**
4. **for SUs in CRN** $i = 1$ to N **do**
SU i share the sensing results with others and list the potential coalitions. Suppose the current coalitional partition $\mathcal{T}_n = \{S_1, \dots, S_{|\mathcal{T}_n|}\}$. There exists N possible coalitional partitions $\mathcal{T}_n{}^1, \dots, \mathcal{T}_n{}^N$.
5. **end for**
6. 1) Calculate spatial correlation
for coalitions $k = 1$ to $|\mathcal{T}_n|$ **do**
for SUs in coalition S_k $i = 1$ to n_k **do**
Calculate $C_i(S_k)$, and $\boldsymbol{C} = \{C_1(S_k), \dots, C_{n_k}(S_k)\}$, by Eq.(5), and find out MUs by Eq.(5) and Eq.(6) to find out MUs
end for
end for
7. 2) Calculate energy consumption
for coalitions $k = 1$ to $|\mathcal{T}_n|$ **do**
for SUs in coalition S_k $i = 1$ to n_k **do**
Calculate $E_i^D(S_k)$, and E $= \{E_1^D(S_k), \dots, E_{n^k}^D(S_k)\}$ from Eq.(8)
end for
end for
8. **Step 2: Coalition Repartition:**
1) If SU i decides whether to join to another coalition based on Eq.(11), update $\mathcal{H}$.
2) If S_k decides to merge with another coalition partition by Eq.(12), update $\mathcal{H}$
9. **Repeat**
Step 1 and Step 2
Untill
Find the optimal coalition partition $\mathcal{T}_{\mathrm{n}}^* = \arg\ \max_{\mathcal{T}_{\mathrm{n}} \in \mathrm{T}} \mathrm{V}(\mathcal{T}_{\mathrm{n}})$

4. Optimal Power Allocation with Malicious users Attacks

SUs access the idle channels belong to the PUs based on the sensing results, and optimize the power allocation to achieve a higher efficiency of the spectrum resource while limiting the performance degradation cause to PUs. Specifically, in this paper, SSDF attack of MUs disrupts the decision-making of FC and affects the power allocation in CRN. So, we should consider MUs in the power allocation process.

In this paper, SU i decides to access channel based on the sensing results, thus the data transmission time of SU i is given by $T - \tau_s - \tau_c$, where τ_s is the sensing time, τ_c is the information exchanging time between SU i and its neighbors, and T is the length of the frame. For the sake of simplicity, we assume T, τ_s and τ_c are fixed value. The sum rate overall channels of SU i in coalition S_k can be expressed as:

$$R_i(S_k) = \left(\frac{T-\tau_s-\tau_c}{T}\right) P(H_0)\theta_i \sum_{i=1}^{M} r_i^l \tag{13}$$

where r_i^l is the transmission rate of SU i in channel l given by:

$$r_i^l = \log_2(1 + \frac{P_i^l G_{i,B}^l}{N_0}) \tag{14}$$

where P_i^l is the transmit power of SU $i \in S_k$ in channel l, $G_{i,B}^l$ is the channel gain between SU i and SBS over channel l. N_0 is the variance of the Gaussian noise in channel l. The $P(H_0)$ is the prior i knowledge of the status of the PU. θ_i is the willing factor, which shows the probability of SU i to join in the MUs detection process. In our scheme, the SU i can decide whether to join in the MUs detection process based on the tradeoff between the achievable rate

and the energy consumption. To achieve the social benefit and promote SUs participate in the MUs detection process, compensation rule is used to allows SUs which join in the MUs detection obtain higher opportunity to access the idle channel. Let will factor θ_i equals to the access probability of SU *i* of idle channel, the SU *i* which did not contribute in MUs detection will be excluded to use the idle channels belong to the PU.

On the one hand, the total power allocation of SU *i* in all channels should not exceed a limit power constraint P_{max}, thus we have:

$$\sum_{i=1}^{M} P_i^l \le P_{max}, \quad \forall i, l \tag{15}$$

On the other hand, notice that FCC claims that there should be a power mask on opportunistic transmissions even the channels are detected to be idle. In order to effectively protect the PU from harmful interference, the interference power constraint can be formulated as follows:

$$P_i^l G_{i,PU}^l \le \Gamma^l, \quad \forall i, l \tag{16}$$

where $G_{i,PU}^l$ is the channel gain between SU *i* and PU over the channel *l*, Γ^l is the maximum interference power could be acceptable by PU over the channel *l*.

In this paper, we aim at maximizing the total utility of SUs by considering the detection probability of MUs and the energy consumption. The detection probability of MUs and the energy consumption are increasing functions with the number of SUs. Focusing on mitigating malicious users attacks, where the percentage of MUs < 50% we maximize the utility of the CRN, and balance the tradeoff between $E_i^D(S_k)$ and $D_i(S_k)$ of SU i in S_k. The normalized expression is used here to ensure the value of each part is in an order of magnitude. The power allocation optimization problem based on malicious users detection can be described as optimization problem P1:

$$\max_{P_i^l, P_d^M, n_k} \; U = \sum_{k=1}^{|\mathcal{T}_n|} \sum_{i=1}^{n_k} \left(\frac{R_i(S_k)}{R_{max}} + \frac{E_i^U(S_k)}{E_{max}} + v_i(S_k, \mathcal{T}_n) \right)$$

$$s.t. \quad C_1: \sum_{i=1}^{M} P_i^l \le P_{max} \tag{17}$$

$$C_2: P_i^l G_{i,PU}^l \le \Gamma^l \tag{18}$$

$$C_3: \sum_{k=1}^{|\mathcal{T}_n|} n_k = N \tag{19}$$

$$C_4: P_i^l \ge 0 \tag{20}$$

$$C_5: D_0 \le P_d^M(S_k) \le 1 \tag{21}$$

where $v_i(S_k, \mathcal{T}_n)$ is the utility of SU i joint energy consumption and the MU detection probability in S_k at coalition partition $\mathcal{T}_n$, particularly $v_i(S_k, \mathcal{T}_n) = v(S_k, \mathcal{T}_n)$ due to the non-transferable character of coalition formation game. n_k is the number of SUs in S_k, $|\mathcal{T}_n|$ is the number of coalitions at iteration *n*, R_{max} in the maximum achievable rate of SU i. $D_0 = 0.8$ is the lowest bound for the detection probability of MUs. $E_i^U(S_k)$ is energy consumption for information transmission from SU *i* to SBS in uplink of S_k.

The problem P1 is a multi-variables optimization problem which is NP hard. The objective function of optimization problem P1 consists of three parts: sum-rate of SUs, the probability detection of MUs and energy consumption.

In order to solve the problem, we use alternating optimization method [26], which can get optimal value of multi-variables by an alternative manner. Firstly, MUs detection step, we use the proposed CMD algorithm to find the optimal coalition partition $\mathcal{T}_n^* = \arg\ max_{\mathcal{T}_{n \in T}} V(\mathcal{T}_n)$, calculate the optimal MUs detection probability $P_d^{M*}(S_k)$ and the number of S_k n_k^* based on an initial transmit power of SU *i* $P_i^l(0)$. Secondly, the power allocation optimization step, we

can use the Lagrange dual decomposition method to get the optimal transmit power P_i^{l*} based on the $P_{d,i}^{M*}(S_k)$ and n_k^* of optimal coalition partition $\mathcal{T}_{\mathrm{n}}^*$ obtained from the previous MUs detection step. Repeat these two steps till convergence.

Based on the MUs detection steps, the probability detection of MUs $P_{d,i}^{M}(S_k)$ and the energy consumption $E_i^D(S_k)$ of MUs detection of SU $i \in S_k$ at $\mathcal{T}_{\mathrm{n}}^*$ have been calculated, thus $v_i(S_k, \mathcal{T}_{\mathrm{n}})$ can be considered as a constant and in the following we optimize the transmit power of SUs in CRN. Therefore, in the power allocation step, optimization problem P1 can be expressed as problem P2:

$$\begin{aligned} &\max_{P_i^l} U = \sum_{k=1}^{|\mathcal{T}_{\mathrm{n}}^*|} \sum_{i=1}^{n_k^*} \left(\frac{R_i(S_k)}{R_{max}} + \frac{E_i^U(S_k)}{E_{max}} + v_i(S_k, \mathcal{T}_{\mathrm{n}}^*)\right) \\ &s.t.\ \ C_1,\ C_2,\ C_3 \end{aligned} \tag{22}$$

To solve the problem P2 effectively, we focus on the optimal power of SU *i* in coalition S_k and the objective function of P2 can be written as:

$$U_i = F_{1,i} \sum_{l=1}^{M} r_i^l + F_{2,i} \tag{23}$$

where $F_{1,i} = \left(\frac{T-\tau_s-\tau_c}{T}\right) P(H_0)\theta_i$ and $F_{2,i} = \frac{E_i^U(S_k)}{E_{max}} + v_i(S_k, \mathcal{T}_{\mathrm{n}}^*)$,Therefore, the original optimization problem P1 can be transformed to a convex optimization problem with respect to P_i^l. Notably, the solution of the dual problem and the original problem has a gap zero based on its slater's condition according to [27]. The Lagrangian dual of problem P2 is given as:

$$\begin{aligned} L\left(P_i^l, \alpha, \boldsymbol{\mu}\right) = F_{1,i} \sum_{l=1}^{M} \log_2\left(1 + \frac{P_i^l G_{i,B}^l}{N_0}\right) + F_{2,i} \\ -\alpha\left(\sum_{l=1}^{M} P_i^l - P_{max}\right) - \sum_{l=1}^{M} \mu_l \left(P_i^l G_{i,PU}^l - \Gamma^l\right) \end{aligned} \tag{24}$$

where α and vector $\boldsymbol{\mu} = [\mu_l]_{l=1}^{M}$ are the dual variables associated with the transmit power constraint Eq.(13) and the interference power constraint given in Eq.(14) respectively.
If all constraints of optimization problem as P2 are satisfied, the optimal solution does exist according to the convex optimization theory. The optimal power allocation P_i^{l*} can be expressed as:

$$P_i^{l*} = \left[\frac{F_{1,i}}{\ln 2(\alpha + \mu_l G_{i,PU}^l)} - \frac{N_0}{G_{i,B}^l}\right] \tag{25}$$

Proof The details of the proof is given in Appendix B.

We outline the MUs detection based power allocation (MPA) algorithm in **Table 2**.

Table 2. MUs detection based power allocation (MPA) algorithm

MUs detection based power allocation (MPA) algorithm
1. Initialization: $n = 0, t_1 = 0, t_2 = 0$, $P_i^l = 0$, $P_{d,i}^M = 0$, $E_i^D = 0$
2. Repeat
for $i = 1{:}\,N$ **do**
1) The MUs detection step:
Find $P_{d,i}^{M*}$, E_i^{D*} by using the CMD algorithm.
Update $P_{d,i}^M(n+1) = P_{d,i}^{M*}$, $E_i^D(n+1) = E_i^{D*}$

2) The optimal power allocation step:

for $l = 1: M$ **do**

Update μ_{l,t_1+1} by $\mu_{l,t_1+1} = \mu_{l,t_1} + a_1(P_i^l G_{i,PU}^l - \Gamma^l)$

If $\mu_{l,t_1+1} < 0$, set $\mu_{l,t_1+1} = 0$ and stop; Otherwise, stop when $|\mu_{l,t_1+1} - \mu_{l,t_1}| \leq \epsilon_1$.

Update α_{t_2+1} by $\alpha_{t_2+1} = \alpha_{t_2} + a_2(\sum_{l=1}^{M} P_i^l - P_{max})$

If $\alpha_{t_2+1} < 0$, set $\alpha_{t_2+1} = 0$ and stop; Otherwise, stop when $|\alpha_{t_2+1} - \alpha_{t_2}| \leq \epsilon_1$

Find P_i^{l*} by Eq.(25).

end for

Update $\mathbf{P}_\mathrm{i}(\mathrm{n}+1) = \mathbf{P}_i^*$, $\mathbf{P}_\mathrm{i} = [P_i^l]_{l=1}^{M}$

Untill

$|P_{d,i}^M(\mathrm{n}+1) - P_{d,i}^M(\mathrm{n})| \leq \epsilon_2$, $|E_i^D(\mathrm{n}+1) - E_i^D(\mathrm{n})| \leq \epsilon_2$ and

$|\mathbf{P}_\mathrm{i}(\mathrm{n}+1) - \mathbf{P}_\mathrm{i}(\mathrm{n})| \leq \epsilon_2$, $n = n+1$ stop

end for

3. Output the optimal utility U_i^* and calculate the optimal utility of CRN U^*.

Where $a_1 > 0$ and $a_2 > 0$ are the step size, and $\epsilon_1 > 0$ and $\epsilon_2 > 0$ are given constants.

5. Simulation Results

In this section, we present numerical simulation results to assess the performance of the proposed CMD and MPA algorithm. In the simulations, we consider a $5km \times 5km$ square area and one PU is located at the center, $N = 100$ SUs are randomly distributed around the PU. The remaining parameters are varied in the given range to compare the performance of the proposed algorithms with different algorithms in the literatures under different conditions. We focus on the performance of the CMD algorithm in energy consumption of MUs detection $E_i^D(S_k)$ and the detection probability of MUs $P_{d,i}^M(S_k)$, and the MPA algorithm in the power allocation utility of the whole CRN with different maximal transmission power P_{max}, the number of idle channel N_c and willing factor θ. Simultaneously, we compare the performance of the CMD algorithm with random coalition based MUs detection (RCMD) algorithm, centralized MUs detection (CD) algorithm [13] and cooperative neighboring cognitive radio nodes (COOPON) algorithm [10]. Based on the performance of the three algorithms above, we consider the performance of the MPA algorithm with random coalition MUs detection based power allocation (RMPA) algorithm and centralized MUs detection based power allocation (CMPA) algorithm.

Fig. 2 shows the energy consumption of MUs detection in CMD algorithm and CD algorithm in both sparse scenario (SS) and dense scenario (DS). In SS, there are 4 SUs per km square and 16 SUs per km square in DS. For both of these two cases, the energy consumption of MUs detection of CMD and CD algorithm increase as the number of SUs increase. Especially, the proposed CMD algorithm yields a considerable energy consumption reduction with respect to the CD algorithm. Due to the total distance between SUs in DS is shorter than in SS, the energy consumption of the proposed CMD algorithm is higher in SS than DS.

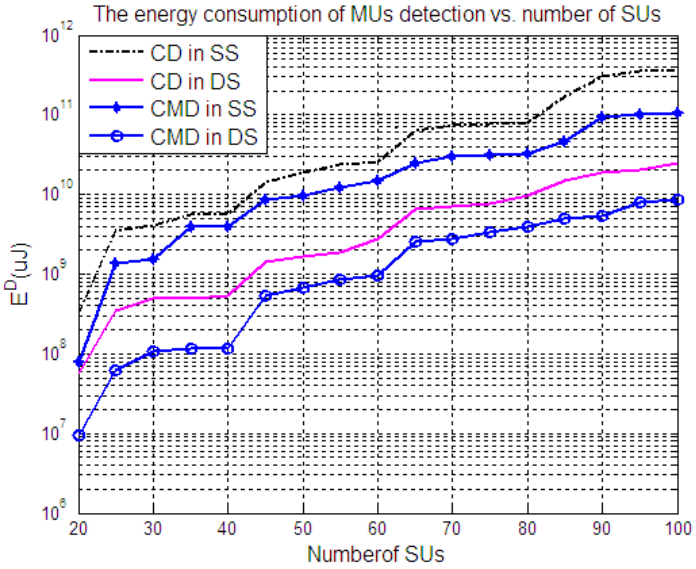

Fig. 2. The energy consumption of MUs detection vs. SUs

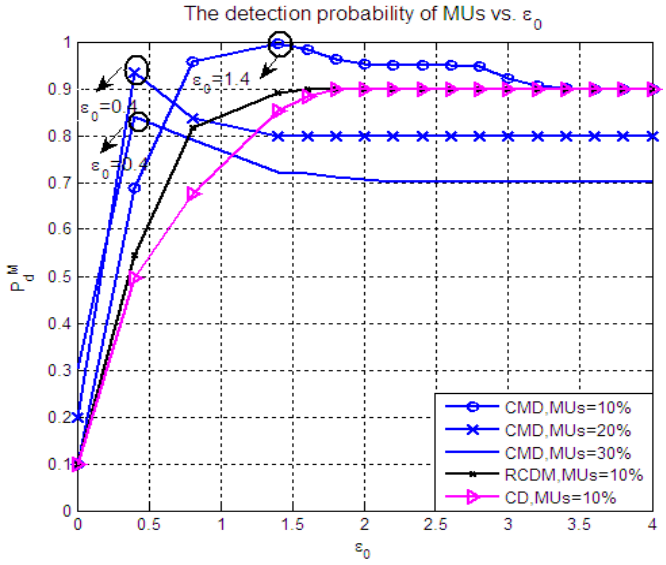

Fig. 3. The detection probability of MUs vs. ε_0

In **Fig. 3**, we compare the detection probability of MUs P_d^M as a function of threshold ε_0 for CMD, RCMD and CD algorithm, and the percentage of MUs ranges from 10% to 30%. According to the result, there exists the optimal threshold ε_0 where the probability of detection MUs is maximized for three algorithms. Benefit from coalition formation game, the proposed CMD algorithm is robust as compared with the RCMD and CD algorithms, more than 80% percent of MUs still can be detected with the increase of threshold ε_0.

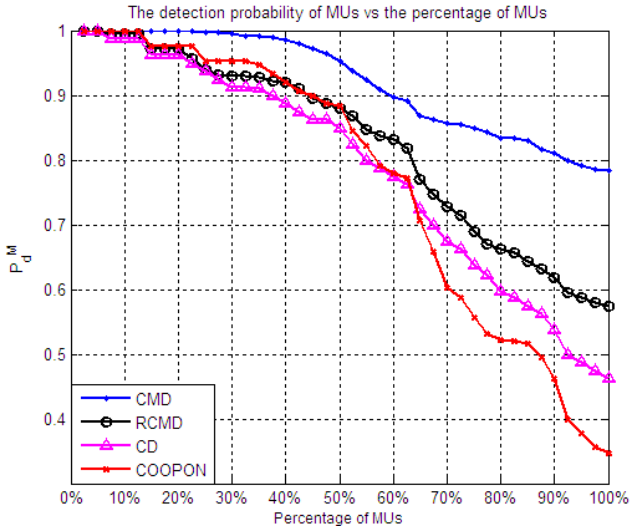

Fig. 4. Detection probability of MUs vs the percentage of Mus

Fig. 4 shows that as the percentage of MUs increases, the P_d^M of CMD, RCMD, CD and COOPON algorithm decrease. For the first three algorithms, ε_0 is used to detect MUs in HC. When the percentage of MUs is more than 50%, which is in SC, we use double threshold to make the final decision of the first three algorithms. It is because the spatial correlation of SUs is mainly influenced by the received power of MUs, which cause a tiny difference of the spatial correlation difference between SUs and MUs and increase the difficulty to detect MUs. Nevertheless, compared with RCMD and CD algorithm, the P_d^M of the proposed CMD algorithm is highest. The COOPON algorithm focuses on comparing the report of channel of the neighboring SUs to detect MUs. With the increasing of the percentage of MUs, more and more neighboring SUs report false report of channel, which increase the difficulty of the comparing process and decrease P_d^M. Due to use of the different thresholds in HC and SC and coalition game, the P_d^M of the proposed CMD algorithm is better than the COOPON algorithm.

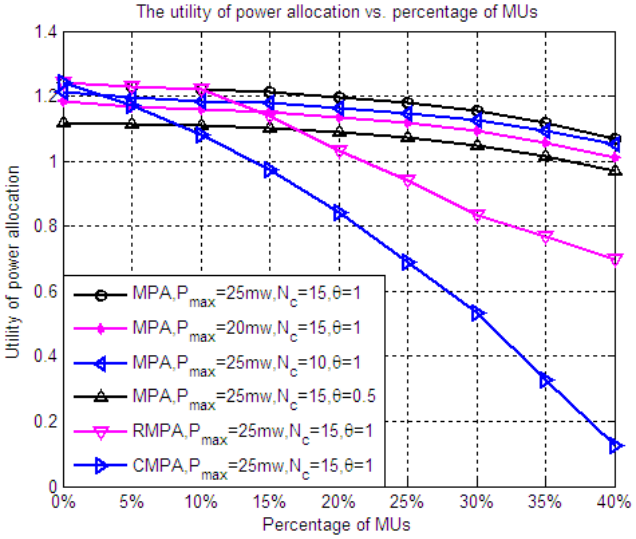

Fig. 5. The utility of power allocation vs. percentage of MUs

Fig. 5 demonstrates the total utility of power allocation versus the percentage of MUs with different P_{max}, N_c and θ for MPA , RMPA and CMPA algorithms, where the transmit power constraint P_{max} ranges from $20mw$ to $25mw$ and the number of idle channels N_c changes from 10 to 15. For the three algorithms, the utility decreases for different P_{max} and N_c with increasing percentage of MUs. In addition, the proposed MPA achieves higher utility compared with RMPA and CMPA algorithm when the willing factor $\theta = 1$. However, when the willing factor $\theta = 0.5$, the total utility of MPA algorithm decreases, which indicates that if only 50% SUs join in the MUs detection scheme will cause severer influence to the performance of the whole system. Notably, even when $\theta = 0.5$, the proposed MPA algorithm can achieve higher utility compared with the RMPA algorithm when the percentage of MUs > 17.5% of the whole CRN. According to the results, the proposed MPA algorithm is quite efficient in an unreliable environment, even half of the SUs participate in MUs detection the total utility is higher than other algorithms.

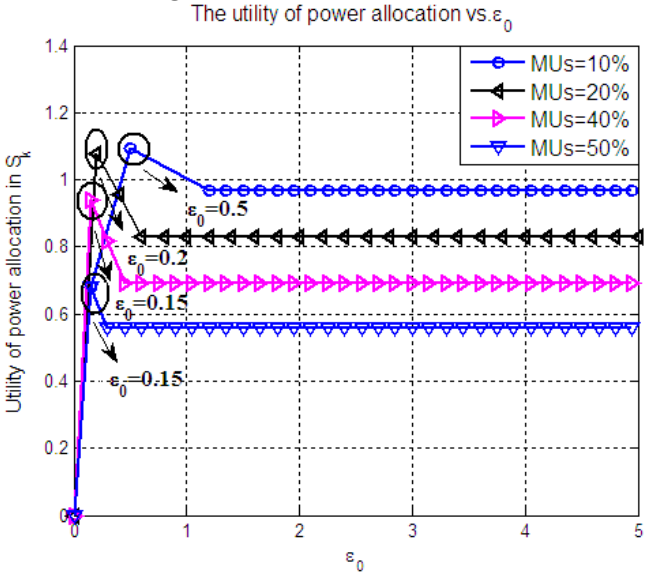

Fig. 6. The utility of power allocation vs. ε_0

Fig. 6 represents that the utility of S_k as a function of the detection threshold ε_0 with different percentage of MUs, where the percentage of MUs ranges from 10% to 50% and $P_{max} = 25mw$, $N_c = 15$ and $\theta = 1$. Generally, the utility of power allocation in S_k decreases as the percentage of MUs increases, since MUs detection becomes more difficult as the percentage of MUs increases. In addition, when the percentage of MUs in S_k is 50%, half of the SUs are MUs, the proposed MPA algorithm still can work properly.

6. Conclusion

In this paper, we firstly propose a coalition based malicious users detection (CMD) algorithm to detect the malicious user in the CRN. The Geary'C theory is used in the proposed CMD algorithm to get the spatial correlations between SUs in the same coalition, and detected the MUs by the difference between them. In addition, we analyze the power allocation problem with MUs attack and propose a MUs detection based power allocation (MPA) algorithm, the proposed MPA algorithm composed of three parts: sum-rate of CRN, the MUs detection probability and the energy consumption of MUs detection. The multi-variables optimization

problem can be solved by alternating optimization method and divided into two sub-problems: the MUs detection and the optimal power allocation. In the MUs detection step, by the CMD algorithm we can obtain the MUs detection probability and the energy consumption of MUs detection. In the optimal power allocation step, we use the Lagrange dual decomposition method to obtain the optimal transmission power of each SU and achieve the maximum utility of the whole CRN. Finally, we highlighted the benefit of using our MPA algorithm comparing to the RMPA and CMPA algorithm in literatures. In the future work, we could improve the performance of SSDF attack in the CRN from three aspects: 1) multiple spectrum bands sensing, SUs need to sense the presence of many PUs simultaneously; 2) more types of MUs, high sensing probability and low sensing probability of MUs will be considered separately; 3) considering more characteristic, more characteristic about the MUs detection algorithm in the CRN will be studied, such as the receiver operating characteristic, algorithm complexity and so on.

7. Appendix

Appendix A: Stability of Coalition Formation Games

We prove the stability by contradiction. Considering the energy consumption of MUs detection E_i^D, n_k the number of SU i in S_k and the number of coalitions available for SU i is limited. Furthermore, according to the record set $\mathcal{H}$, SU i is prevented from revisiting previously joined coalitions again. Therefore, convergence of the algorithm is guaranteed. In other words, there must be a final coalition partition for the proposed CMD algorithm. If the final partition is D-stable, arbitrary initial coalition partitions can reach D-stable because of the operations in the proposed coalition game are based on Pareto order. Otherwise, we assume the final partition of the proposed game is not D_{hp}-stable, a partition $\mathcal{T}'$ is formed by using merge-split operation to leave the partition exist. It illustrates that a new partition will be generated and the proposed game cannot stop, which conflict with the assumption and the fact that the algorithm is converged, thus, the partition $\mathcal{T}'$ do not exist and the final partition is D_{hp}-stable. Hence, the proposed CMD algorithm can reach stability.

Appendix B: The proof of Eq.(25)

In order to judge on convexity of the optimization problem P2, we analyze the character of second partial derivative $\frac{\partial^2 L(P_i^l,\alpha,\boldsymbol{\mu})}{\partial^2 P_i^l}$ as follow:

$$\frac{\partial L(P_i^l,\alpha,\boldsymbol{\mu})}{\partial P_i^l} = \frac{F_{1,i}}{\ln 2(N_0+P_i^l G_{i,B}^l)} - \alpha - \mu_l G_{i,PU}^l \tag{26}$$

$$\frac{\partial^2 L(P_i^l,\alpha,\boldsymbol{\mu})}{\partial^2 P_i^l} = \frac{F_{1,i} {G_{i,B}^l}^2}{\ln 2(N_0+P_i^l G_{i,B}^l)} \tag{27}$$

It is clear that $F_{1,i} = \left(\frac{T-\tau_s-\tau_c}{T}\right) P(H_0)\theta_i > 0$, we get $\frac{\partial^2 L(P_i^l,\alpha,\mu)}{\partial^2 P_i^l} \leq 0$ and the problem P2 is convex. The Karush-Kuhn-Tucker (KKT) conditions of problem P2 can be expressed as follow:

$$\frac{\partial L(P_i^l,\alpha,\boldsymbol{\mu})}{\partial P_i^l} = \frac{F_{1,i}}{\ln 2(N_0+P_i^l G_{i,B}^l)} - \alpha - \mu_l G_{i,PU}^l = 0$$
$$\sum_{i=1}^{M} P_i^l - P_{max} \leq 0 \tag{28}$$

$$\alpha\left(\sum_{l=1}^{M} P_i^l - P_{max}\right) = 0 \quad (29)$$

$$P_i^l G_{i,PU}^l - \Gamma^l \le 0 \quad (30)$$

$$\mu_l\left(P_i^l G_{i,PU}^l - \Gamma^l\right) = 0 \quad (31)$$

The multipliers α and $\boldsymbol{\mu} = [\mu_l]_{l=1}^{M}$ are calculated by using the subgradient algorithm, which converges to the optimal solution of convex problems within a small range by using a constant step length. According to the subgradients [28], α and μ_l are given by:

$$\mu_{l,t_1+1} = [\mu_{l,t_1} + a_1(P_i^l G_{i,PU}^l - \Gamma^l)]^+ \quad (32)$$

$$\alpha_{t_2+1} = [\alpha_{t_2} + a_2(\sum_{l=1}^{M} P_i^l - P_{max})]^+ \quad (33)$$

where $a_1 > 0$ and $a_2 > 0$ are the step size, t_1 and t_2 are the iteration number, $[x]^+ \triangleq max(0, x)$. From KKT condition above, it is observed that the optimal solution satisfies $\frac{\partial L(P_i^l, \alpha, \boldsymbol{\mu})}{\partial P_i^l} = 0$. Then $\frac{\partial L(P_i^l, \alpha, \boldsymbol{\mu})}{\partial P_i^l} = \frac{F_{1,i}}{\ln 2(N_0 + P_i^l G_{i,B}^l)} - \alpha - \mu_l G_{i,PU}^l = 0$, we have

$$P_i^l = \frac{F_{1,i}}{\ln 2(\alpha + \mu_l G_{i,PU}^l)} - \frac{N_0}{G_{i,B}^l} \quad (34)$$

Since the transmit power cannot be negative, thus the optimal power allocation strategy is $P_i^{l*} = max\left[\frac{F_{1,i}}{ln2(\alpha+\mu_l G_{i,PU}^l)} - \frac{N_0}{G_{i,B}^l}, 0\right]$ and Eq.(25) is proved.

References

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Communications*, vol. 6, no.4, pp. 13-18, August 1999. Article (CrossRef Link)

[2] Xiaoge Huang, Liping Chen, Qianbin Chen and Bin Shen, "Coalition formation based malicious user detection scheme in cognitive radio networks," in *Proc. of 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications*, pp.1415-1419, August 30-September 2, 2015. Article (CrossRef Link)

[3] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," *IEEE Communications Surveys and Tutorials*, vol. 15, no.1, pp. 428-445, February, 2013. Article (CrossRef Link)

[4] H. Redwan, A. Suwon and K. Kim, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks," in *Proc. of 2008 Japan-China Joint Workshop on Frontier of Computer Science and Technology*, pp. 3-9, December 27-28, 2008. Article (CrossRef Link)

[5] R. Chen, J. M. Park and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25-37, January, 2008. Article (CrossRef Link)

[6] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han and J. Wang, "Byzantine Attack and Defense in Cognitive Radio Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342-1363, August, 2015. Article (CrossRef Link)

[7] A. Vempaty, K. Agrawal, H. Chen and P. Varshney, "Adaptive learning of Byzantines' behavior in cooperative spectrum sensing," in *Proc. of 2011 IEEE Wireless Communications and Networking Conference*, pp.1310-1315, March 28-31, 2011. Article (CrossRef Link)

[8] Kun Zeng, Przemyslaw Pawelczak, and Danijela Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226-228, March, 2010. Article (CrossRef Link)

[9] G. Ding, Q. Wu, Y. Yao, J. Wang and Y. Chen, "Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions," *IEEE Signal Processing Magazine*, vol. 30, no. 4, pp. 126–136, July, 2013. Article (CrossRef Link)

[10] M. Jo, L. Han and D. Kim, "Selfish attacks and detection in cognitive radio ad-hoc networks," *IEEE Network*, vol. 27, no. 3, pp. 46-50, May, 2013. Article (CrossRef Link)
[11] A. Min, K. Shin and X. Hu, "Secure cooperative sensing in IEEE 802.22 WRANS using shadow fading correlation," *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1434-1447, October, 2011. Article (CrossRef Link)
[12] P. Kaligineedi, M. Khabbazian and V. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488-2497, August, 2010. Article (CrossRef Link)
[13] Changlong Chen, Min Song, ChunSheng Xin and Mansoor Alam, "A robust malicious user detection scheme in cooperative spectrum sensing," in *Proc. of 2012 IEEE Global Communications Conference*, pp. 4856-4861, December 3-7, 2012. Article (CrossRef Link)
[14] P. D. Mankar, G. Das and S.S. Pathak, "A centralized method for optimal power allocation in cognitive radio networks," in *Proc. of 2013 IEEE Globecom Workshop*, pp. 385-390, December 9-13, 2013. Article (CrossRef Link)
[15] F. Ahmed, O. Tirkkonen, AA. Dowhuszko and M. Juntti, "Distributed power allocation in cognitive radio networks under network power constraint," in *Proc. of 2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pp. 492-497, June 2-4, 2014. Article (CrossRef Link)
[16] Xiaoge Huang, Baltasar Beferull-Lozano and Carmen Botella, "Quasi-Nash Equilibria for Non-Convex Distributed Power Allocation Games in Cognitive Radios," *IEEE Transactions on Wireless Communications*. vol. 12, no. 7, pp. 3326-3337, July, 2013. Article (CrossRef Link)
[17] Xiaoge Huang, Fan Zhu, Yongxu Zou and Qianbin Chen, "Dynamic Base Station Assignment and Resource Allocation in MIMO CR Small-cell Networks," in *Proc. Of 2014 14th International Symposium on Conmunications and Information Technologies*, pp. 61-65, September 24-26, 2014. Article (CrossRef Link)
[18] L. Anselin, "Local indicators of spatial association—LISA," *GEOGRAPHICAL ANALYSIS*, vol. 27, no. 2, pp. 93-115, April 1995. Article (CrossRef Link)
[19] Y.-C. Liang, Y. Zeng, E. C. Y. Peh and A. T. Hoang, "Sensing throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*. vol. 7, no. 4, pp. 1326-1337, April, 2008. Article (CrossRef Link)
[20] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in *Proc. of 2012 31st IEEE International Conference on Computer Communications*, pp. 900-908, March 25-30, 2012. Article (CrossRef Link)
[21] C. S. Hyder, B. Grebur, LiXiao, M. Ellison, "ARC: Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks," *IEEE Transactions on Mobile Computing*, vol. 13, no.8, pp.1707-1719, August, 2014. Article (CrossRef Link)
[22] E. Björnson, L. Sanguinetti, J. Hoydis, and M. Debbah, "Optimal design of energy-efficient multi-user MIMO systems: Is massive MIMO the answer?" *IEEE Transactions on Wireless Communications*, vol. 14, no. 6, pp. 3059-3075, June, 2015. Article (CrossRef Link)
[23] W. Saad, Z. Han, M. Debbah, A. Hjorungnes and T. Basar, "Coalitional game theory for communication networks," *IEEE Signal Processing Magazine*, vol. 26, no. 5, pp. 77–97, September, 2009. Article (CrossRef Link)
[24] W. Saad, Z. Han, M. Debbah and A. Hjorungnes, "Coalitional Games for Distributed Collaborative Spectrum Sensing in Cognitive Radio Networks," in *Proc. of 28th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies*, pp. 2114-2122, April 19-25, 2009. Article (CrossRef Link)
[25] K. Apt and A. Witzel, "A generic approach to coalition formation," *International Game Theory Review*, vol. 11, no. 3, pp. 347-367, September, 2009. Article (CrossRef Link)
[26] Xiaoge Huang and Baltasar Beferull-Lozano, "Non-cooperative power allocation game with imperfect sensing information for cognitive radio," in *Proc. of 2012 IEEE International Conference on Communications*, pp. 1666-1671, June 10-15, 2012. Article (CrossRef Link)

[27] S. Singh, P. Teal, P. Dmochowski and A. Coulson, "Interference management in cognitive radio systems — A convex optimization approach," in *Proc. of 2012 IEEE International Conference on Communications*, pp. 1884-1889, June 10-15, 2012. Article (CrossRef Link)
[28] Xu Yongjun and Zhao Xiaohui, "Optimal power allocation for multiuser underlay cognitive radio networks under QoS and interference temperature constraints," *China Communications*, vol. 10, no. 10, pp. 91-100, October, 2013. Article (CrossRef Link)

Xiaoge Huang received Ph.D. degree (with first honors) in the Institute of Robotics and Information & Communication Technologies (IRTIC) at the University of Valencia, in 2013. She is now an associate professor of Chongqing University of Posts and Telecommunications (CQUPT). Her research interests include convex optimization, centralized and decentralized power allocation strategies, game theory, cognitive radio networks, and multiuser MIMO systems.

Liping Chen received the B.S. degree in electronics and communication engineering from the Chongqing University of Posts and Telecommunications, Chongqing, 2016. Her research interests include spectrum sensing and power allocation in cognitive radio networks, wireless communications, game theory, and network security.

Qianbin Chen dean of the school of electronics and communication engineering, University of Posts and Telecommunications. His research interests include personal communication, multimedia information processing and transmission, next generation networks, LTE-Advanced heterogeneous cellular networks.

Bin Shen recieved B.E., M.Sc. and Ph.D. degree in electronic engineering in 2000, 2005 and 2010, respectively. He is now a professor of Chongqing University of Posts and Telecommunications (CQUPT). His current research interests include signal processing in multi-antenna system and cognitive radios.