Coalition Formation Based Malicious User Detection Scheme in Cognitive Radio Networks

Xiaoge Huang, Liping Chen, Qianbin Chen, Bin Shen
School of Communication and Information Engineering
Chongqing University of Posts and Telecommunications, Chongqing, China
Email: {Huangxg, Chenqb, Shenbin}@cqupt.edu.cn, chen-li-ping@hotmail.com.

Abstract—In cognitive radio networks, a critical issue is to exploit the spectrum holes based on spectrum sensing while avoiding interference to the primary users. However, the reliability of sensing is uncertain. In order to increase the probability to access the channel, cognitive users may report false detection results and become malicious users (MUs), which could significantly degrade the performance of spectrum sensing. In this paper, we proposed an energy efficient MUs detection algorithm which is able to perform coalition-based cooperative detection and spatial correlation with Geary'C theory to maximize the probability of MUs detection. The problem is reformulated as a coalition game with the theoretical certification of its stability. Simulation results show that our algorithm is able to achieve a significant improvement while saving the energy in the MUs detection process compared with other algorithms in the literature.

I. INTRODUCTION

Cognitive Radio (CR) is an emerging technology to improve spectrum utilization in flexible and efficient way. A core problem in Cognitive Radio Networks (CRNs) is to exploit the spectrum holes, in which unlicensed secondary users (SUs) need to sense the spectrum of licensed primary users (PU) and decide whether it can be used or not. However, the local sensing result of a single SU is vulnerable to fading and shadowing over wireless channels. To overcome this problem, cooperative spectrum sensing has been proposed, in which sensing results of multiple SUs are combined to achieve better performance. Collaborative sensing techniques are well studied in [1]–[5], the main approaches can be grouped into three categories based on the share methods of sensing data: centralized, relay-assisted, and distributed [1]. In CRNs, due to the uncertain in sensing process, SUs are divided into two types: honest SUs (HUs), which report the real sensing results, and malicious SUs (MUs), denoted in [2], which send false sensing to increase the chance of using the spectrum and decrease the performance of a cooperative sensing system. Detection of MUs depend on the type of MUs and the testing environment. In [3], the authors proposed a scheme to detect single MU in centralized spectrum sensing. Although the scheme can differentiate a HU and a MU, it is not applied to multiple MUs scenario. In [4], Min et al. proposed to use the shadow fading correlation to detect MUs, which reduces the impact from MUs on the performance of distributed cooperative sensing. A detection scheme proposed in [5] utilizes the spatial information of CR sensors, which can be applied in the scenario with a few MUs. Most of the approaches in the literatures considered for MUs detection in centralized manner which would limit the scalability of these approaches. In our previous work, we proposed a decentralized MUs detection scheme based on dynamic reputation of each SU [2].

In this paper, we consider a CRN with both HUs and MUs. In order to detect the MUs from all the SUs, we proposed an energy efficient MUs detection algorithm which is able to perform coalition-based detection and spatial correlation to maximize the probability of MUs detection. In particular, we formulate the algorithm as a coalition formation game, and analyze its properties and certificate its stability theoretically. To deal with inherent relation with each SU, the Geary'C theory in [6] is used to calculate the spatial correlation of each SU, which contribute to the spatial correlation. The MUs detection is based on the distinction of spatial correlation between HUs and MUs. Numerical results show that the proposed algorithm is able to yield a significant improvement while saving the energy in the MUs detection process compared to other algorithms in the literature.

The rest of this paper is organized as follows. In Section II, we present the cooperative sensing system model with MUs. A coalition-based for MUs detection algorithm is proposed in Section III. IV presents performance evaluation and finally the conclusions are drawn in Section V.

II. SYSTEM MODEL

Consider a CRN composed of one PU and N SUs. We assume that all SUs and PU are stationary in transmission, and the reliability of all SUs is uncertain. Thus, the SUs may have malicious or cheating behavior in order to gain their profit and become MUs. Cooperative approach is an efficient way to improve the accuracy of spectrum sensing, where each SU senses spectrum individually and makes the final decision in a cooperative manner. We assume all SUs adopt energy detection to detect the presence of the PU [7], and the probability of detection and false alarm for SU i are given by $P_{d,i}$, $P_{fa,i}$ respectively:

\[
P_{d,i} = P\{Y > \lambda|H_1\} = Q((\lambda - \gamma_i - 1)/\sqrt{\tau f s})
\]

\[
P_{fa,i} = P\{Y > \lambda|H_0\} = Q(\tau f s)
\]

(1)
where hypothesis $H_0$ represents the absence of PU while $H_1$ states the present. $Y$ denotes the obtained statistic energy from PU, $\lambda$ denotes the decision threshold of the energy detector, $\gamma_i$ is the received SNR of SU $i$ from PU, $f_s$ represents the sampling frequency and $\tau$ means the sensing time. The noise is assumed to be independent and identically distributed circularly symmetric complex Gaussian, $CN(0,1)$. The received power of SU $i$ from PU can be expressed as:

$$P_i = P_t - (10\mu \log_{10}(d_i/d_o)) + G_i(dB)$$

where $P_t$ is the transmit power of PU, $\mu$ is the path-loss exponent, $d_i$ is the distance from PU to SU $i$, and $d_o$ is the reference distance, $G_i$ is the log-normal shadowing coefficient which can be accounted by $e^{X_i}$ where $X_i \sim N(\mu,\sigma^2)$. Our goal is to find out MUs who sent the false sensing results in the cooperation scheme to maximize their probability to access the idle channel belong to PU. In order to minimize the interference between SUs as well as increase the reliability of detecting MUs, in the paper, we propose a coalition-based malicious user detection algorithm (CMD). The proposed CMD scheme joint coalition formation (CF) and spatial correlation (SC), which could detect MUs efficiently with low energy consumption. The details are given in the following section. An example of the coalition formation structure is shown in Fig.1.

### III. MALICIOUS USERS DETECTION SCHEME

MUs change dynamically during different detecting period. In order to find MUs in CRNs, the proposed scheme can be sum up in five steps during a detecting period: 1) Local Sensing: all SUs use energy detector to sense the presence or absence of PU independently. Note that there are honest SUs as well as MUs. 2) Discovery: SUs share their local sensing result with their neighbors and form coalitions under a certain rule. 3) Spatial Correlation (SC), in this step, we first calculate the spatial correlation of each SU by Geary’s theory and choose a SU which has the least spatial correlation as the coalition head. Then the coalition head will decide MUs in the coalition under certain rule. 4) Detection Probability and Energy Consumption (DPEC), we calculate the detection probability of MUs based on the decision of MUs detection and energy consumption of detecting MUs in each coalition $S$. 5) Adjustment, we use the Pareto order [10] to adjust the coalitions based the detection probability of MUs and energy consumption of detecting MUs.

#### A. Discovery

Based on local sensing results from Eq.(1). Each SU needs to discover potential cooperation SUs under the following condition:

- $P_{d,i}$ and $P_{d,j}$ respectively are the sensing results of SU $i$ and SU $j$, if $|P_{d,i} - P_{d,j}| \leq \alpha$, SU $i$ and SU $j$ can combine with together.

#### B. Spatial Correlation

In a coalition, there are MUs which report false sensing results in order to join in the coalition and increase the probability to access the idle channel belong to PU. In this case, MUs may decrease the performance of cooperative sensing. In this paper, we consider a Geary’s theory to detect MUs in each coalition. Geary’s is one of the spatial statistics indicators which is useful to find the difference in each coalition. In fading environment, sensing results from nearby HUs are similar. Therefore, based on Geary’s theory, the HUs have smaller spatial correlation compared with MUs in each coalition. We choose a SU which has the least spatial correlation as the coalition head. Assume MUs report false sensing results and really report the information of other SUs, the coalition head can make a true decision. We use Geary’s to measure the spatial correlation of SU $i \in S$ which is the autocorrelation between SU $i$ and its neighboring SUs in the coalition $S$ denoted as $C_i(S)$:

$$C_i(S) = \frac{\sum_{j=1}^{n} w_{ij}(P_i - P_j)^2}{\frac{1}{n} \sum_{j=1}^{n} (P_j - \bar{P})^2}$$

where $n$ is the number of SUs in coalition $S$, $P_i$ and $P_j$ are received power of SU $i$ and SU $j$ from PU. $\bar{P}$ is the average received power of SUs in coalition $S$. $w_{ij} = d^{-1/2}_{ij}$ is the weight factor of spatial correlation between SU $i$ and SU $j$, and $d_{ij}$ is the distance between SU $i$ and SU $j$.

To deal with the difference density of MUs, we consider two kinds of scenario with respect to the percentage of MUs in each coalition, that are, Honest case and Greedy case:

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

$$D_i(S) = \begin{cases} 
1 & \text{if } C_i(S) > \varepsilon_0 \\
0 & \text{if } C_i(S) \leq \varepsilon_0 
\end{cases}$$

- Greedy Case (GC): the percentage of MUs is more than 50% of a coalition.

$$D_i(S) = \begin{cases} 
1 & \text{if } \varepsilon_1 < C_i(S) < \varepsilon_2 \\
0 & \text{if } C_i(S) \geq \varepsilon_2 \text{ or } C_i(S) \leq \varepsilon_1 
\end{cases}$$

where $D_i(S) = 1$ denotes SU $i$ is considered as a MU, otherwise $D_i(S) = 0$. $\varepsilon_0$, $\varepsilon_1$ and $\varepsilon_2$ are decision thresholds. The mean value of the received power is critical for calculating the spatial correlations of SUs in a coalition. In HC, the mean value of the received power is the dominate factor for spatial correlation of SUs and the difference between the
The proposed algorithm is shown in Algorithm 1.

Algorithm 1 Coalition based Malicious User Detection Algorithm (CMD)

1: Initialization:
   MUs and SUs are randomly distributed around a PU.
2: LocalSensing:
   SUs obtain the sensing results by Eq.(1).
3: Discovery:
   SUs share the sensing results with their potential neighbors and form the initialized coalition \( T = \{ T_1, ..., T_l \} \).
4: Spatial Correlation:
5: for coalitions \( j = 1 \) to \( l \) do
6:   for SUs in coalition \( S_j \) \( i = 1 \) to \( n \) do
7:     Calculate \( C_i(S_j) \), and \( C = \{ C_1(S_j), ..., C_n(S_j) \} \) from Eq.(3) and choose the SU \( i \) which has \( \min(C_1(S_j)) \) as the coalition head \( H_j \).
8:   end for
9: end for
10: Adjustment:
   Using merge and split rule to adjust the \( T = \{ T_1, ..., T_l \} \) until converge.
Repeat:
11: a) \( \mathcal{M} = \text{Merge}(\mathcal{T}) \) coalitions in \( \mathcal{T} \) by using merge rule.
12: b) \( \mathcal{T} = \text{Split}(\mathcal{M}) \) coalitions in \( \mathcal{M} \) by using split rule.
13: Untill merge-and-split converges, when reach Partition Stability, forming a set of coalitions \( S = \{ S_1, ..., S_l \} \).

C. Detection Probability, Energy Consumption

The detection probability of MUs and energy consumption of detecting MUs in coalition \( S \) are two important factors which should be taken into consideration in coalition formation. During the Spatial Correlation, the coalition head can find MUs in coalition \( S \), then we can calculate the detection probability of MUs in coalition \( S \) as follows:

\[
P_d^n(S) = \frac{n_d}{n}
\]

where \( n \) is the number of SUs in coalition \( S \), \( n_d \) is the number of SUs which are accurately detected. The total energy consumption of coalition \( S \) can be given as follows:

\[
E(S) = \sum_{i=1}^{n} E_i(S)
\]

where \( n \) is the total number of SUs in coalition \( S \), \( E_i(S) \) is SU \( i \)'s energy consumption in coalition \( S \). For SU \( i \)'s energy consumption in coalition \( S \) contributes to two parts:

- Energy consumption for transmitting information \( E_t^i(S) \):
  SU \( i \) sends its spatial correlation to \( H \), which is the head of \( S \).
- Energy consumption for receiving information \( E_r^i(S) \):
  coalition head \( H \) transmits the final decision to SU \( i \) in coalition \( S \).

Thus, the total energy consumption of SU \( i \in S \) in MUs detection is:

\[
E_i(S) = E_t^i(S) + E_r^i(S)
\]

where \( E_t^i(S) \) and \( E_r^i(S) \) are given by:

\[
E_t^i(S) = \begin{cases} 
  k_0\epsilon_0 + \alpha_1(d_i)^{\alpha_1} & \text{if } d_i < d_{co} \\
  k_0\epsilon_0 + \alpha_2(d_i)^{\alpha_2} & \text{if } d_i \geq d_{co}
\end{cases},
E_r^i(S) = k\epsilon_0
\]

where \( \epsilon_0 \) is the energy consumption of transmitting or receiving per data packet, \( k \) is the number of data packets, \( d_i \) is the distance between SU \( i \) and PU, \( d_{co} \) is the reference distance, \( \alpha_1, \alpha_2, \beta_1, \beta_2 \) are constants in the transmission models [9]. The proposed algorithm is shown in Algorithm 1.

IV. COALITION FORMATION GAMES

We formulate the coalition formation as a coalitional game \( G = \{ \mathcal{N}, \mathcal{V}, \mathcal{M} \} \) with a nontransferable utility (NTU):

- Players: \( \mathcal{N} \) as is the set of all SUs.
- Action Set: \( \mathcal{M} = \{ \text{Merge, Split} \} \) is common action set of SUs, which includes two actions Merge and Split.
- Utility: \( \mathcal{V} \) is a mapping for every coalition \( S \subseteq \mathcal{N} \), \( \mathcal{V}(S) \) is a closed convex subset of \( \mathbb{R}^S \) that contains the utility vectors of SUs in coalition \( S \).

A. Utility

For coalitional game \( G = \{ \mathcal{N}, \mathcal{V}, \mathcal{M} \} \), the payoff \( \phi_i(S) \) of a coalition \( S \) is equal to the utility \( v(S) \), where \( \phi_i(S) \) is the utility of SU \( i \) when acting as part of \( S \), given as [11]:

\[
V(S) = \{ \phi \subseteq \mathbb{R}^S | \phi_i(S) = v(S) \ \forall i \in S \}
\]

To improve the detection probability of MUs, as well as reducing the energy consumption in MUs detection process, the utility \( v(S) \) of a coalition \( S \) which is a function that gets the tradeoff between the detection probability of MUs and energy consumption can be defined as:

\[
v(S) = \begin{cases} 
  \frac{P_d^n(S)}{E(S)} & \text{if } n_m \in \mathcal{R} \\
  0 & \text{if } n_m \notin \mathcal{R}
\end{cases}
\]

where \( P_d^n(S) \) is the detection probability of MUs in coalition \( S \), \( n_m \) is the number of SUs per coalition can hold. \( \mathcal{R} \) is the optimal set of \( n_m \). It is clear that energy consumption increase with the increasing number of SUs per coalition while the probability of detection and false alarm will increase simultaneously.

B. Action Set

According to [12], we use two rules based on Pareto order to adjust the structure of coalitions, namely: merge and split. The SUs in coalition \( S \) will choose their actions modify their spatial correlations of HUs and MUs is clear. In GC, there are more MUs than HUs, which increase the difficulty of MUs detection. Since the distinction between the spatial correlations of HUs and MUs is tiny. To overcome this problem double threshold \( \varepsilon_1 \) and \( \varepsilon_2 \) is used here to make the final decision. The optimal value of threshold \( \varepsilon_0, \varepsilon_1, \varepsilon_2 \) can be obtained by exhausted search method.
partition based on following two rules to optimize the structure of coalitions and maximize the total utility.

- **Merge Rule:** Merge any set of coalitions \( \{S_1, ..., S_i\} \), where \( \bigcup_{j=1}^{i} S_j \supset \{S_1, ..., S_i\} \), therefore \( \{S_1, ..., S_i\} \rightarrow \bigcup_{j=1}^{i} S_j \).
- **Split Rule:** Split any coalition \( \{U_{j=1}^{l} S_j\} \), where \( \{S_1, ..., S_i\} \supset \bigcup_{j=1}^{l} S_j \), therefore \( \bigcup_{j=1}^{l} S_j \rightarrow \{S_1, ..., S_i\} \).

where \( l \) is the total number of coalitions in a partition. \( A = \{A_1, ..., A_l\} \) and \( B = \{B_1, ..., B_l\} \) are different partitions of SUs, \( A \supset B \) means that the payoff of each SU of partition \( A \) is more than partition \( B \). SUs will keep adjusting the partition of coalitions by using merge and split rule until stability.

**C. Partition Stability**

The result of the game can form a network partition which consist of independent coalitions of SUs. To demonstrate the stability of the proposed game, we introduce the basic conception of defection function \( D \), \( D_{hp} \), \( D \)-stable and \( D_{hp} \)-stable as follow [12].

**Definition 1.** A defection function \( D \) is the function that can map each partition \( T \) of \( N \) into a group of collections in \( N \). A partition \( T = \{T_1, ..., T_l\} \) of \( N \) is \( D \)-stable if no players intend to leave \( T \) when the players who leave can only form the collections allowed by \( D \).

If the partition \( T \) 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 [12]:

- For each pair of disjoint coalitions \( S_1 \) and \( S_2 \) in \( T \), \( S_1 \cup S_2 \supset S_1 \cup S_2 \) is satisfied.
- For the partition \( T = \{T_1, ..., T_l\} \), a coalition \( S' \subset N \) formed by SUs belonging to different \( T_i \in T \), which can be regarded as \( T \)-incompatible. If the partition \( T \) is \( D \)-stable, all \( T \)-incompatible coalitions should satisfy \( S' \cap T_i, \forall i \in \{1, ..., l\} \supset S' \).

**Definition 2.** A defection function \( D_{hp} \) is the function that can map a partition \( T \) of \( N \) into a group based on merge-split operation. A partition \( T = \{T_1, ..., T_l\} \) 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, linear and rule is merge-split. We use the following lemma to demonstrate the stability of CMD algorithm.

**Lemma.** For a arbitrary coalition formation game, the comparison relation is monotonous, transitive, irreflexive and linear and rule is merge-split, can reach the optimal \( D \)-stable partition if such a partition exists. Otherwise, the final network partition is \( D_{hp} \)-stable [12].

**Proof.** If the \( D \)-stable partition exits, arbitrary initial partitions can reach \( D \)-stable because of the operations in the proposed game are based on Pareto order. Otherwise, if there were not \( D \)-stable partitions, we assume the final partition \( T \) of the proposed game is not \( D_{hp} \)-stable, a partition \( T' \) formed by using merge-split operation to leave the partition \( T \) exits. It illustrates that merge-split rule is satisfied but the proposed game can not stop, which conflict with the assumption, so the partition \( T' \) do not exit and the final partition \( T \) is \( D_{hp} \)-stable. So, the proposed algorithm can reach stability.

**V. SIMULATION RESULTS**

In this section, we present numerical simulation results to assess the performance of the proposed CMD 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 CMD algorithm with different algorithms in the literatures under different conditions. We focus on the performance of the algorithms in energy consumption and the probability to find MUs in coalitions. We compare the performance of three algorithms: a) coalition based MUs detection algorithm (CMD), which is proposed in this paper. b) random coalition based MUs detection algorithm (RCMD). c) centralized MUs detection algorithm (CD).

The sensing time \( \tau \) and sample frequency \( f_s \) of energy detector are \( 10ms \) and \( 6MHz \). The transmit power \( P_t \) of PU is \( 100mW \). The D-value \( a \) of sensing results of SUs which can merge together is \( 0.2 \). The energy consumption per data packet \( e_0 \) is \( 50nJ \). In the transmission model [9], the reference distance \( d_{co} = 86.4m \) and the transmission factors \( \alpha_1, \alpha_2, \theta_1, \theta_2 \) are \( 10^{-10}, 10^{-11}, 2 \) and \( 4 \). The optimal set of the number of SUs per coalition \( R \) is \([3,10]\). The range of the threshold
In general, the optimal $P_{d}^{m}$ of coalition $S$ decreases as the percentage of MUs increases, which explains that detecting MUs becomes more difficult as the percentage of MUs increases. In addition, when the percentage of MUs in coalition $S$ is 50%, which leads to the greedy case, more than half of the SUs are MUs, the proposed CMD algorithm still can find the MUs efficiently and it is suitable for both GC and HC. Figure 5 shows that as the percentage of MUs increases, the $P_{d}^{m}$ of CMD, RCMD and CD algorithm decreases. Furthermore, $P_{d}^{m}$ sharply reduced around the percentage of MUs is 50%, which is the boundary between HC and GC. For the three algorithms, $P_{d}^{m} > 80\%$ in HC, whereas $P_{d}^{m} < 50\%$ in GC. When the percentage of MUs is more than 50\%, that is in GC, although we use double threshold to make the final decision, the spatial correlation of SUs is mainly influenced by the received power of MUs, the spatial correlation difference between SUs and MUs are tiny which increase the difficulty to detect MUs. Compared with RCMD and CD algorithm, the $P_{d}^{m}$ of the proposed CMD algorithm is highest.

VI. CONCLUSION

In this paper, we proposed the coalition-based cooperative sensing for malicious user detection algorithm (CMD) to detect malicious users efficiently in decentralized manner. Furthermore, we reformulated the problem as a coalition game and proved the stability of the game theoretical. Finally, we highlighted the benefit of using our algorithm comparing to the random and centralized malicious users detection algorithm.

REFERENCES