IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 19, 2018, accepted February 18, 2019, date of publication February 22, 2019, date of current version March 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2901200

Privacy-Aware Crowdsourced Spectrum Sensing and Multi-User Sharing Mechanism in Dynamic Spectrum Access Networks

XIAOHUI LI[1,2], QI ZHU[1,2], AND XIANBIN WANG[3], (Fellow, IEEE)

[1]Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[2]Engineering Research Center of Health Service System Based on Ubiquitous Wireless Networks, Nanjing University of Posts and Telecommunications (Ministry of Education), Nanjing 210003, China
[3]Department of Electrical and Computer Engineering, University of Western Ontario, London, ON N6A 5B9, Canada

Corresponding author: Qi Zhu (zhuqi@njupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61571234 and Grant 61631020, and in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX18_0886.

ABSTRACT Dynamic spectrum access (DSA) emerging as an effective way of improving the utilization of the scarce spectrum has attracted great attention in the communication field. A key challenge in DSA is to perform an efficient spectrum sensing and sharing mechanism. In this paper, aiming at achieving a maximal spectrum utilization, we propose a privacy-aware crowdsourced spectrum sensing and multi-user sharing mechanism for DSA. Particularly, in the sensing stage, the advanced mobile crowd sensing is adapted to economically provide sufficient candidate sensing helpers for a sensing requestor. Considering the individual rationality and energy consumption, an incentive mechanism based on both monetary and social motivation is designed to motivate the finial participations of the sensing helpers. Moreover, with the increasing attention to individual privacy, a social network and location-based k-anonymity grouping algorithm are proposed to prevent each helper's privacy being attacked by the malicious requestor or mobile users. Then, for a sensing requestor, aiming at achieving a target detection performance with minimal payment, a truthful reverse auction-based winning group selection algorithm is designed. Furthermore, in the transmitting stage, a realistic scenario is considered where multiple transmitters may discover the same idle spectrum based on sensing helpers' detections and will transmit data simultaneously. Thus, we model this problem as a potential-game-based multi-user transmission mechanism where all the transmitters act as game players and will jointly adjust their transmission powers to maximize the global throughput. Accordingly, we also take advantage of an improved differential evolution algorithm for obtaining a better equilibrium solution in a decentralized way. Both the theoretical analysis and the simulation results prove the rationality and superiority of our proposed algorithms.

INDEX TERMS Privacy aware, mobile crowd sensing, incentive mechanism, dynamic spectrum access, game theory.

I. INTRODUCTION

With the increasingly scarce spectrum, dynamic spectrum access [1] (DSA) has always been a significant technique to improve the spectrum utilization. Numerous state-of-the-art researches [2]–[4] have studied the DSA from various aspects. One of the crucial challenges in DSA is to accurately detect the status of the primary user (PU) and establish an efficient transmission scheme. In realistic scenario, the detection result from a single user is unreliable due to the deep fading or shadow effect in wireless communications. Thus to guarantee the detection performance, the cooperative spectrum sensing [5], [6] should be adopted, however, almost all existing related works assume that there are sufficient secondary users (SU) to cooperate when a PU's state is needed to detect. Yet, it's not rational enough in realistic scenario where maybe only a limited number of SUs exist during the current timeslot and will not sense the spectrum if they have

The associate editor coordinating the review of this manuscript and approving it for publication was Bhaskar Prasad Rimal.

no data transmitting, which will eventually incur a limited sensing coverage, and finally degrade the cooperative sensing performance. Mobile crowd sensing (MCS) [7] emerging as a new sensing paradigm can provide sufficient candidate sensing users in spatial domain, where not only the existing SUs but also the widespread mobile users equipped with various sensors can participate in the cooperative sensing process.

Yet considering the energy consumption and individually rational property, idle mobile users may be unwilling to contribute themselves to the cooperative sensing process unless satisfied profits can be obtained to compensate their costs. In another word, incentive mechanism [8] is necessary in MCS to motivate the cooperative sensing participation of the widely distributed mobile users. There have been plenty of papers taking advantage of the incentive mechanism and MCS to solve kinds of problems [9]–[13]. Papers [9] and [10] adopt the monetary incentive mechanism to motivate the crowd sensing users, where the participating users will be paid a certain amount of monetary rewards [8]. Specifically, Ying *et al.* [9] design an expected utility maximization based pricing mechanism aiming at motivating and selecting users to perform the crowd-sensed radio mapping process. And a geographical position conflicting MCS system with two user-selection algorithms is proposed in [10] to prevent the sensing platform buying duplicated sensory data with multiple payments. Beyond that, with the rapid development of communities and social networks, the nonmonetary incentive, namely the social network incentive [11], has also emerged as another efficient way to motive a sufficient number of participants. In particular, a sensing requestor can recruit a crowd of reliable users within his social network, i.e., the friends, to help complete crowdsourcing tasks. And these friends are willing to join in the tasks mainly due to the following achieved profits: developing relationships with other members, obtaining good reputations, and getting immediately identical helps in the future. A number of works [12]–[14] have adopted the social incentive into kinds of situations. Paper [12] proposes a credible crowd sensing task assignment model based on social relationship cognition and community detection. Paper [13] balances the conflicts between sybil attack and heterogeneous effect of participants in the proposed social network based crowdsourcing incentive mechanism. In research [14], the time-sensitive and Sybil-proofness problems are considered in the social network-based MCS system.

Nonetheless, to the best of our knowledge, there are few applications of MCS and incentive mechanism in the DSA field [15]–[17]. Ding *et al.* [15] focus on improving quality of the spectrum sensing data obtained from crowd sensing users. While Gao *et al.* [16] propose a two-tier game based incentive mechanism where the database directly motivates secondary users to participate in the spectrum sensing. And in [17], a crowdsourcing-based spectrum sensing is utilized to periodically collect the spectrum availability information over a large geographic area and finally a radio environment map can be constructed and efficiently maintained. Above researches consider only positive profit incentives, i.e., extra monetary or social-network benefits, for mobile sensing users in MCS based spectrum sensing. However, with increasing attention to privacy preservation, the crowd sensing users may still refuse to contribute their data in the case that the information provided by themselves will expose their individual privacies and even result in malicious attacks. In a word, besides profits given to the participating users, the protection of their individual privacy should also be considered.

Recently, the privacy protection in MCS has attracted high attention in numerous researchers [18]–[21]. Wang *et al.* [18] utilize the k-anonymity to reduce the risk of location-privacy disclosure for crowd sensing users. Yet the group aggregation is mainly based on users' locations, and the existing of malicious group members is not considered. Lin *et al.* [19] propose two frameworks for privacy preservation in auction based incentive mechanism. Zhang *et al.* [20] design an incentive mechanism to maximize the fusion center's aggregation accuracy by quantizing crowd sensing users' privacy preserving levels and characterizing their impacts on the aggregation accuracy. Paper [21] focuses on the location privacy in the crowdsourced spectrum sensing scenario and presents a novel framework, consisting of two different schemes under distinct design objectives and assumptions, for a service provider to select participants in a differentially privacy-preserving manner. Above related works focus on protecting a participant's privacy only from either other crowd sensing users or the service requestor, whereas an integrated and more reliable privacy preservation mechanism considering potential attacks from both mobile users and the requestor should also be studied.

On the other hand, besides the study for cooperative spectrum sensing, there are also plenty of researches focusing on the transmission scheme for dynamic spectrum sensing [22], [23]. These works consider only one transmitter in an idle spectrum and mainly concentrate on the individual sensing time and transmission power optimization. However, in realistic situation, there usually exist a certain number of transmitters who discovery an idle spectrum at the same time and will transmit data in the same transmitting time slot, which will consequently incur inevitable interference among these transmitters and at last degrade the global transmission performance. Thus some effective methods need to be adopted to maximize the utilization of the idle channel.

Based on above analysis, in this paper, we propose a privacy-aware crowdsourced spectrum sensing and multi-user sharing mechanism for achieving an efficient spectrum utilization in DSA. Specifically, aiming at achieving a maximal spectrum utilization, transmitters need to firstly acquire the accurate status of the licensed user by recruiting a certain number of mobile users. Thus in our paper, we adopt the MCS to provide a spatial-domain guarantee for each transmitter, so that he can select an optimal number of sensing helpers from the widespread mobile users. Furthermore, considering the energy consumption and the risk of privacy leak,

we propose an incentive mechanism based on both monetary incentive and privacy preservation. Particularly, the privacy preservation mechanism is designed based on the k-anonymity algorithm where the candidate sensing helpers can protect their individual information from both malicious sensing members and sensing requestor by forming groups based on their social networks and relative locations. Moreover, when stepping into the transmitting stage, a potential game based multi-user spectrum sharing mechanism is proposed aiming at maximizing spectrum utilization and the global throughput. The main contributions in this paper are listed as follows:

- We adopt advanced MCS into cooperative spectrum sensing scenario, where a widely spread mobile users equipped with kinds of sensors can be regarded as a sufficient number of candidate sensing helpers for each sensing requestor. Beyond that, taking account of inevitable sensing consumption and individual rationality, we also propose a reverse auction based monetary incentive mechanism to motivate the participation of mobile users, where positive profits, i.e., a certain amount of monetary reward, can be obtained by each winning helper. Furthermore, the essential economic properties of the reverse auction mechanism are proved. Compared with existing works related to cooperative spectrum sensing, our proposed mechanism provides a spatial-domain guarantee for the accuracy of spectrum detection with less facility configuration costs and greater flexibility.
- With the increasing attention to individual information, we propose a k-anonymity based privacy preservation mechanism where each sensing helper can hide its individual information within a k-size sensing group and the sensing data can be reported in group rather than directly to the requestor, which effectively prevents individual privacy being attacked by a malicious requestor. Furthermore, to avoid malicious members existing in a sensing group, we exploit both social inventive and location proximity as the grouping rule, where each sensing helper will form a group firstly with the reliable ones who are within its social network and the location proximity rule is used to prune away surplus members or add new members. Compared with existing works related to k-anonymity privacy preservation, our proposed mechanism protects each sensing user's individual privacy from both malicious requestor and malicious members within the same group by exploiting the social network and location proximity based grouping rule.
- Compared with existing works that focus on the jointly optimization of sensing time and transmission power for one transmitter, we consider a realistic transmission scene where multiple transmitters may detect the absence of the PU simultaneously and will transmit data in the same idle spectrum. Aiming at decreasing the mutual interference among transmitters and maximizing global throughput in current spectrum, a potential game based multi-user spectrum sharing mechanism is proposed, where all transmitters act as game players and need to jointly adjust their own transmission power strategies to achieve the optimization objective. Furthermore, in order to obtain a better Nash Equilibrium, we design an improved differential evolution algorithm, where compared with the typical best response dynamic algorithm, a larger scale of initial points and candidate solutions can be searched and hence a better equilibrium solution can be obtained.

The rest of the paper is organized as follows. Section II describes the proposed system model. Section III gives a detailed illustration about proposed privacy-aware crowdsourced spectrum sensing mechanism and section IV analyses the multi-user transmitting mechanism. Then the simulation results are presented in section V and the conclusions are showed in section VI.

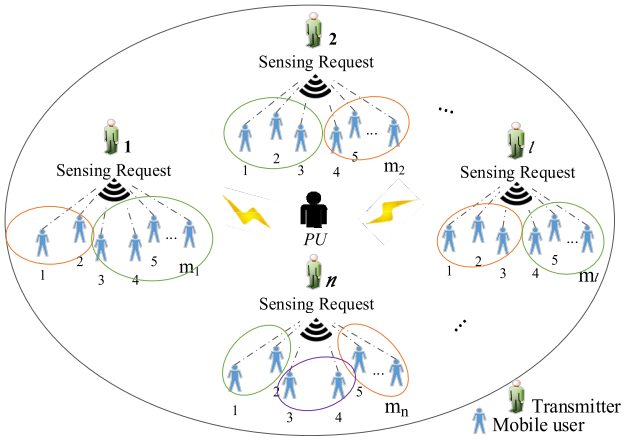

FIGURE 1. System model.

II. SYSTEM MODEL

As illustrated in Fig 1, there exist multiple transmitters (also called requestors) $\mathbf{N} = \{1, 2, \ldots, l, \ldots, n\}$ and a crowd of widespread mobile users in our proposed system model. Ultimately, the objective is to achieve a maximal global throughput for all transmitters simultaneously transmitting in a utilized spectrum by scheduling their transmitting power. Nevertheless, before accessing the spectrum, each transmitter $l, \forall l \in \mathbf{N}$ needs to firstly obtain an accurate status about the PU with the cooperative helps of mobile users. While for each idle mobile user j (also regarded as a candidate sensing helper), who is interested in helping the transmitter l, further incentives are needed for him to eventually participate in the sensing process and contribute his sensing data, due to the inevitable sensing costs and the risk of privacy leak. Hence, in cooperative sensing part, the payment minimization optimization is formulated where each transmitter aims at achieving a target detection performance with minimal payment to the cooperative sensing helpers. Note that we assume a realistic scene with incomplete information where each transmitter has no idea about the existence of other

transmitters when he decides to sense or transmit in current spectrum during the same transmission slot. As a result, in the spectrum sensing part, transmitters cannot form a cooperative sensing coalition and hence need to respectively recruit a certain number of sensing helpers to achieve their own target detection performance.

Specifically, we illustrate the system model as follows in two parts. The first part is the privacy-aware crowdsourced spectrum sensing model where for each mobile user, aiming at protecting privacy by hiding individual information among other users with similar characteristics, he will firstly join or form a k-size sensing group. Hence the crucial information, such as cost and detection data, will be reported in groups rather than in individual. Consequently, the sensing requestor cannot distinguish any user's individual information from the other members within the same k-size group. Then based on the reported grouping information, the sensing requestor will select an optimal set of winning groups to achieve a target detection performance and meanwhile provides each winning helper with a non-negative monetary profit. This process can be formulated as a total payment minimizing optimization problem subject to a target detection performance constraint. Then the second part is the multi-user spectrum sharing model where several transmitters may utilize the same vacant spectrum to transmit their data in the same time slot and inevitable interference exist among these transmitters. Hence aiming at achieving a best utilization of the idle spectrum by adjusting each transmitter's transmission power, a global throughput maximizing optimization problem is formulated. Before proceeding further, we list the main notations used in the following sections in Table 1.

TABLE 1. List of main notations.

Symbol	Definition
$\mathbf{N}$	Set of transmitters
l	Index of the transmitter
H_l	Set of sensing helpers of transmitter l
j	Index of the sensing helper
CG_l	Set of candidate sensing groups of transmitter l
NG_l	The number of candidate sensing groups of transmitter l
g	Index of the sensing group
N_g	The number of members within sensing group g
WG_l	Set of winning groups of transmitter l
wg	Index of the winning sensing group
wj	Index of the winning sensing helper

A. CROWDSOURCED SPECTRUM SENSING MODEL

During the spectrum sensing part, aiming at acquiring a better detection performance, each transmitter l needs to recruit a proper number of sensing helpers participating in the cooperative sensing process. As a result, each requestor l will announce the sensing request to all mobile users within his transmitting range. And when receiving the quest, the idle mobile users who are interested in performing the cooperative sensing task will be regarded as candidate sensing helpers within the set $H_l = \{1, \ldots, j, \ldots, m_l\}$. In order to select an optimal set of sensing winners from H_l, the transmitter l has to acquire the individual information from each helper j, such as the sensing cost and local sensing data. However, due to the malicious probability of sensing requestor and the personal privacy leakage risk, the sensing helpers will be reluctant to report their own information directly to the requestor and even drop out of the candidates set.

Hence in our proposed crowdsourced spectrum sensing model, we adopt a k-anonymity [24] based privacy preservation mechanism where at least k and no more than $2k-1$ helpers, who have similar characteristics, will form a sensing group and then the sensing cost and sensing data will be reported to the requestor in groups. Namely, the requestor will obtain the necessary information from group rather than directly from an individual helper, which means whether the requestor is malicious or not, he cannot distinguish every member's privacy information from the others in the same group. Furthermore, a bigger k means that each helper can get more anonymous preservation from other members with similar characteristics. As a result, the privacy preservation of each sensing helper can be protected from the sensing requestor. We design the grouping rule based on both social network and users' locations, where each sensing helper will form a group firstly with the ones who are not only in its social network, namely the friends, but also in the same set H_l. And if the number of friends is less than k, the existing members will further consider the strangers who are nearest and haven't joined in any group yet. The details of grouping algorithm will be illustrated in section III.

In particular, in this crowdsourced model, for each transmitter l, all his sensing helpers in H_l, will firstly constitute NG_l candidate sensing groups $CG_l = \{1, \ldots, g, \ldots NG_l\}$ based on proposed grouping rule where the size of each group satisfies $k \leq N_g \leq 2k-1$. Then each group g will compute the group sensing cost c_g and group sensing detection result, i.e., the cooperative detection probability Q_g^d and the cooperative false alarm probability Q_g^f, and then report the group information above to the requestor l. For each group g, the group sensing cost c_g in our proposed model is defined as the maximal individual sensing cost $c_{j,\max}$ multiplied by the number of helpers N_g in this group:

$$c_g = c_{j,\max} \cdot N_g, \quad j \in g \tag{1}$$

The group detection performance, namely the group detection probability and group false alarm probability based on OR fusion rule, is presented as follows:

$$Q_g^d = 1 - \prod_{j \in g} (1 - q_j^d) \tag{2}$$

$$Q_g^f = 1 - \prod_{j \in g} (1 - q_j^f) \tag{3}$$

where the q_j^d and q_j^f are respectively the local detection probability and local false alarm probability of helper $j \in g$ based on the energy detection method [25]:

$$q_j^d = Q((\frac{\varepsilon}{\sigma^2} - \gamma_j - 1)\sqrt{\frac{t_s f}{2\gamma_j + 1}}) \tag{4}$$

$$q_j^f = Q((\frac{\varepsilon}{\sigma^2} - 1)\sqrt{t_s f}) \tag{5}$$

The standard Gaussian Q-function is defined as

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-t^2/2)dt \tag{6}$$

And t_s represents the sensing time, f is sampling frequency, σ^2 is variance of circularly symmetric complex Gaussian noise, and ε is the detection threshold of energy detector. Note that during the sensing slot of transmitter l, all its sensing helpers will take the same time to perform the spectrum sensing task. Meanwhile, $\gamma_j = \frac{w_{PU} h_{PU,j}}{\sigma^2}$ is the received signal-to-noise ratio (SNR) over the link from primary user to user j, where w_{PU} is the transmission power of PU and $h_{PU,j}$ is the path loss between PU and user j.

Aiming at achieving a threshold detection performance with minimal expense, i.e., the incentive payment to all sensing helpers, when receiving the sensing costs and detection data from NG_l groups, the requestor l needs to select an optimal winning group subset WG_l from the candidate group set CG_l. Consequently, we can formulate the winning group selection model as the following optimization problem:

$$\begin{aligned} \Gamma_l(WG_l) = \min & \sum_{wg \in WG_l} r_{wg} \\ s.t.\ & Q^d_{WG_l} \geq \overline{Q}^d_{th} \\ & Q^f_{WG_l} \leq \overline{Q}^f_{th} \end{aligned} \tag{7}$$

where r_{wg} is the reward paid to the winning sensing group wg, $\overline{Q}^d_{th}$ and $\overline{Q}^f_{th}$ is respectively the expected threshold detection probability and threshold false alarm probability. $Q^d_{WG_l}$ is the global sensing detection probability obtained by all the winning groups in WG_l:

$$Q^d_{WG_l} = 1 - \prod_{wg \in WG_l} (1 - Q^d_{wg}) \tag{8}$$

and $Q^f_{WG_l}$ is the corresponding global false alarm probability:

$$Q^f_{WG_l} = 1 - \prod_{wg \in WG_l} (1 - Q^f_{wg}) \tag{9}$$

where Q^d_{wg} and Q^f_{wg} is respectively the group detection probability and group false alarm probability of wg, $\forall wg \in WG_l$.

Consequently, for each sensing helper wj in any winning group wg, its utility function can be represented as follows:

$$u_{wj} = r_{wj} - c_{wj} \tag{10}$$

where r_{wj} is the obtained sensing reward defined as:

$$r_{wj} = \frac{r_{wg}}{N_{wg}}, \quad \forall wj \in wg \tag{11}$$

Namely all the N_{wg} members in the group wg will share the group reward r_{wg} evenly. And c_{wj} is the total cost of helper wj considering both the sensing cost c^s_{wj} and the privacy leak cost c^{py}_{wj} which is inversely proportional to the number of the members in the same group:

$$c_{wj} = c^s_{wj} + c^{py}_{wj} \tag{12}$$

$$c^s_{wj} = c^s_{wj_0} \cdot t_s \tag{13}$$

$$c^{py}_{wj} = \frac{a}{N_{wg}} \tag{14}$$

where $c^s_{wj_0}$ is the unit sensing cost of wj and a is the privacy preservation coefficient.

B. MULTI-USER SPECTRUM SHARING MODEL

When transmitter l makes a decision that the current spectrum is vacant based on the cooperative sensing results from winning helpers, he will immediately transmit his data. However, in reality, there may exist other transmitters who also discover this vacant channel and will transmit data at the same time, which may incur to an inevitable interference between each other and eventually degrades the overall performance of data transmission. Thus in our proposed multi-user data transmitting model, in order to realize a best utilization of the current vacant spectrum, all of the transmitters will jointly adjust their own transmission power until an optimal equilibrium power profile is found to achieve the maximal global throughput of the channel. Before formulating the model, we will firstly give a detailed description about the interference relationship among the transmitters.

For each transmitter, when he transmits data with a certain power, the other ones within his transmitting range will be interfered; and accordingly he will also be interfered by other transmitters if he is located in their transmitting scales. Hence for clarity, we define a correlation set for transmitter l as

$$C_l = B_{l,-} \cup B_{-,l} \tag{15}$$

where $B_{l,-}$ is the set of transmitters who are interfered by user l and $B_{-,l}$ is the set of transmitters who have direct interference on user l, namely user l is located right in their transmitting ranges. Consequently, the non-correlation set of user l, i.e., the other transmitters who have no relationship with l, can be shown as

$$NC_l = \mathbf{N} \backslash C_l \tag{16}$$

where $\mathbf{N} = \{l\} \cup C_l \cup NC_l$.

A transmitter will transmit data if current spectrum is idle and he successfully discoveries it with the probability of $(1 - Q^f_{WG_l})$ based on the detection results of his sensing helpers. Thus based on cooperative detection results and the interference analysis above, we can calculate the throughput of transmitter l as follows:

$$THR_l(p_l, \mathbf{p}_{-l}) = E \cdot (1 - Q^f_{WG_l}) \cdot \log_2(1 + \frac{h_l \cdot p_l}{\sigma^2 + Inf_{B_{-,l}}}) \tag{17}$$

where p_l and h_l is respectively the transmitting power and channel gain of user l and $\mathbf{p}_{-l}$ is the power strategy profile of all transmitters excluding p_l. E is the channel's bandwidth, σ^2 is the noise level, and $Inf_{B_{-,l}}$ means the total interference on transmitter l:

$$Inf_{B_{-,l}} = \sum_{i \in B_{-,l}} h_i \cdot p_i \tag{18}$$

Considering our purpose of maximizing the global throughput by jointly adjusting transmitters' power, the optimization problem can be formulated as:

$$\Pi(\mathbf{p}) = \max \sum_{l \in \mathbf{N}} THR_l(\mathbf{p}) \tag{19}$$

where $\mathbf{p} = \{p_l, \mathbf{p}_{-l}\} = \{p_1, \ldots p_l, \ldots p_n\}$ is power strategy profile of all transmitters in the same vacant spectrum.

III. PRIVACY-AWARE CROWDSOURCED SPECTRUM SENSING MECHANISM

In our proposed crowdsourced spectrum sensing model, aiming at preserving privacy, each sensing helper j will firstly form a sensing group with at least $k-1$ helpers. Then the requestor will select an optimal winning group subset based on the reported group sensing cost and group detection performance, so that he can achieve a target detection performance with minimal total payment to the winning sensing groups. As we can see, the proposed privacy-aware incentive mechanism mainly contains three parts: sensing helper grouping part, winning group selection part and the payment calculation part. Particularly, we design our grouping algorithm based on both social network and location proximity. And we model a reverse auction to analyze the winning group selection part and calculate the payment to winning helpers. We will illustrate the three parts respectively as follows and finally give a detailed proof about economic properties of the proposed reverse auction mechanism.

A. SOCIAL NTEWORK AND LOCATION PROXIMITY BASED GROUPING ALGORITHM

In order to solve the problem that sensing helpers may be reluctant to contribute their data due to the requestor's malicious probability and the risk of individual information leakage, we propose a k-anonymity based privacy-aware mechanism where sensing helpers can form a number of sensing groups whose size satisfy $k \leq N_g \leq 2k-1$ and then report both sensing data and sensing cost in groups rather than directly to the requestor. Specifically, the requestor cannot distinguish the individual information of any member from the others in the same group. Apparently, the grouping rule is the crucial point of the privacy preservation mechanism. Existing k-anonymity based researches [26], [27] mainly focus on the location-oriented user aggregation mechanism but rarely consider that malicious members may disguise themselves to join in a group by lying about their individual information such as their location, which will incur an inevitable attack to not only normal members' privacy but also the reported group data. Considering this issue, we design a novel grouping algorithm in the k-anonymity mechanism, where both social network and location proximity are adopted to provide a double protection of helpers' privacy information.

Specifically, in our proposed grouping mechanism, each sensing helper $j \in H_l, \forall l \in \mathbf{N}$ will give the helpers who are not only in the same helper set H_l but also in his social network, namely the friends in H_l, priorities to form a sensing group with him, so that his privacy information will be protected among his reliable social circle and will not be attacked by malicious users. Meanwhile, when choosing friends in H_l, users' locations will also be considered by helper j. Concretely, the friend who is closest to j will be firstly combined, which is meaningful to prevent the location-privacy disclosure by hiding each helper in a location-proximity group so that an adversary cannot distinguish any member's specific location from the whole group. And, if the number of the friends is less than k, the other strange helpers (also in the same set H_l) who are located at the minimum distance with j and haven't joined in any other groups yet, will be welcomed to be the members of the current group, so that at least k members in a group can be guaranteed. However, for the sake of privacy security, any strange member within a group must not be the head node to collect other members' information or report group data to the requestor. Instead, the only thing a stranger can do is report its information or sensing data to the reliable head node. This mechanism provides a necessary assurance to prevent the strangers tampering the group data or even extracting individual privacy from other reliable members' information. In more details, we note that the proposed grouping algorithm in our system model is a self-organizing and cluster-based grouping process, where each sensing helper decides to form or join in a sensing group by himself based on the social relationship and relative locations with others. After that, when each sensing group is formed, the head node within the group will collect all members' sensing data and then report to the sensing requestor who further makes a decision whether access to the spectrum or not.

We give a detailed example of our proposed grouping mechanism in Fig 2 where the transmitter l, $\forall l \in \mathbf{N}$, announces his sensing request to all mobile users within his transmission range, and the idle users who are interested in participating in the sensing process will be seen as the candidate sensing helpers (i.e., the mobile user 1-13). We assume two social networks (i.e., the user 1-5, user 7, user 10 are in the first social network; the user 6 and user 8 are in the second social network) and three separate users who are not in any social network (i.e., user 9, user 12 and user13) in Fig 2.

Due to the fact that grouping results are irrelevant to the grouping order, without loss of generality, we assume that the grouping process begins from the social network with the most members (i.e., the first social network in Fig 2). Moreover, we also assume that a head node of a group is set as the one nearest to the requestor. This assume is based on the

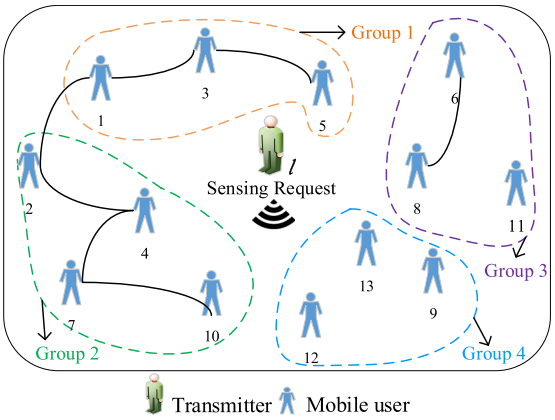

FIGURE 2. An example of proposed grouping mechanism with $k = 3$.

rationality that the nearest one can report his group detection result to the requestor with the shortest transmission distance, namely, with the least information loss. The head node within a social network will decide with whom to form a sensing group based on the social network size. There are three cases:

Case 1: If the number of remaining ungrouping members within a social network is less than k (i.e., the second social network), the nearest strangers to the head node (i.e., user 8) will be welcomed until the number of group members reaches to k (i.e., the user 11 will join in a group 3 with user 6 and user 8).

Case 2: If the number of remaining ungrouping members is more than $2k-1$ (i.e., the first social network), the head node (i.e., user 5) will form a k-size sensing group preferentially with his social members who are nearest to him (i.e., the user 3 and user 1). After completing a group within the social network, the next head nodes among the remaining ungrouping members is selected and uses the same rule to form sensing group, until the number of remaining ungrouping members is more than k and less than $2k-1$.

Case 3: If the number of remaining ungrouping members is more than k and less than $2k-1$, all of them will form a sensing group (i.e., the user 2, user 4, user 7 and 10 form a group 2).

Finally, the rest candidate helpers who have not joined in any sensing group can be seen as the members within a special network and they will use the same rule to form sensing group (i.e., user 9, user 12 and user 13 form group 4). Note that at last the number of remaining sperate users may less than k, thus considering the reality, we assume that they will make a decision, namely participate in the sensing process by forming a new group with other sperate users or giving up the sensing process, based on a random probability.

For all candidate sensing helpers of each transmitter l, we describe the social network and location proximity based grouping algorithm in Algorithm 1, where G_h is the set of helpers who have been in some sensing group, R_h is the remaining helpers who have not been in any group yet, CG_l is

Algorithm 1 Social Network and Location Proximity Based Grouping Algorithm

Initialization:

1. Rearrange the set $H_l = \{1, \ldots, j, \ldots, m_l\}$ as $H_l = SN_1 \cup \ldots SN_i \cup \ldots SN_n \cup SN_{n+1}$, where SN_i, $1 \le i \le n$, represents the ith social-network set, SN_{n+1} is the set of helpers who are not in any social network;
2. Sort all social network sets with a descending order of set size;
3. **for** $i = 1 : n+1$, do
   sort the members within subset SN_i with a descending order of the distance to the requestor;
   end for
4. $CG_l = \emptyset$;

Grouping Operation:

5. **for** $i = 1 : n+1$, **do**
6. **while** $|SN_i| \neq 0$, **do**
7. **if** $(2 \le |SN_i| < k) \& (i \le n) == 1$
   for $x = k - |SN_i|$
   $y = \arg\max_{y \in SN_{n+1}} d(y, SN_i(1))$;
   $g = SN_i \cup \{y\}$; $SN_{n+1} = SN_{n+1} \backslash \{y\}$;
   end for
   $SN_i = \emptyset$;
   end if
8. **if** $(2 \le |SN_i| < k) \& (i = n+1) == 1$
   $\alpha = rand(0, 1)$;
   if $\alpha \ge 0.5$, $g = SN_{n+1}$;
   else break;
   end if
   end if
9. **if** $k \le |SN_i| \le 2k-1$,
   $g = SN_i$; $SN_i = \emptyset$;
   end if
10. **if** $|SN_i| > 2k-1$
   $g = \{SN_i(1:k)\}$; $SN_i = SN_i \backslash g$;
   end if
11. $g \rightarrow CG_l$;
12. **end while**
13. **end for**
14. Return finial candidate sensing group set CG_l.

the finial grouping results and the notation || represents the number of the symbols within the given set. First, in initialization part, we organize the H_l as several existing social network sets and a sperate user set (i.e., line1), and then rank all social network sets with a descending order of set size (i.e., line 2). Line 3 sorts members within each social network with an ascending distance to requestor. Line 7 corresponds to the case 1, line 8 is designed for the remaining members within the set SN_{n+1}. Line 9 and line 10 respectively correspond to the case 3 and case 2. Finally, the eventual grouping result CG_l is achieved.

In a word, the social network and location proximity based grouping algorithm achieves the privacy preservation not only

by guaranteeing a reliable grouping circumstance where each helper can form group firstly with his credible friends; but also by considering users' proximal locations when forming a group with friends or a few strangers, which prevents a malicious requestor distinguishing any member's individual information especially the location-privacy from the whole group. Moreover, the behavioral restrictions to strange members within a group also protect the reliable friend members' privacies to some extent.

B. REVERSE AUCTION AND MARGINAL DETECTION EFFICIENCY BASED GROUP SELECTION ALGORITHM

When sensing helpers form a candidate sensing group set CG_l out of privacy preservation, the corresponding requestor l will then select an optimal winning group subset, i.e., the $WG_l = \{1, \ldots, wg, \ldots\}$, to achieve a target cooperative detection probability and meanwhile minimize his total payment to the winning groups. This process has been modeled as a total payment minimizing optimization problem in equation (7), which is evidently a typical *knapsack problem* [28] and the optimal solution is NP-hard to find due to its combinatorial optimization property.

Thus in order to find a better sub-optimal solution, we design a reverse auction based group selection algorithm where each sensing group firstly calculate its group detection probability Q_g^d and bring up a bidding group cost $bc_g = \sum_{j \in g} bc_j$, then given the provided information the requestor l will select the winning groups based their marginal detection efficiency ME_g, namely if more ME_g a sensing group can obtain, the bigger probability it will be selected as the winning groups. Specifically, the marginal detection efficiency of group $\forall g \in CG_l$ is defined as follow:

$$ME_g = \frac{Q_{WG_l}^d \otimes Q_g^d - Q_{WG_l}^d}{bc_g} \tag{20}$$

where $Q_{WG_l}^d \otimes Q_g^d$ means the global detection probability when adding group g as a new winning group into current winning group set WG_l, $\otimes$ represents the operation in equation (2), while $Q_{WG_l}^d$ is the global detection probability of current winning groups. Requestor l always selects groups into the winning set in the order of descending marginal detection efficiency, until its target global detection probability $\overline{Q}_{th}^d$ is reached.

As we can see, the marginal detection efficiency based selection standard not only considers the bidding cost of a candidate sensing group but also takes account of the improvement of global detection probability that a candidate sensing group can obtain, which is well-matched to the requestor's optimization goal, namely achieving the target detection performance $\overline{Q}_{th}$ with minimal total payment.

For each requestor l, $\forall l \in \mathbf{N}$, the details of the reverse auction and marginal detection efficiency based group selection algorithm is illustrated in Algorithm 2, where Bc is the bidding group cost set of all candidate sensing groups, Q_G^d is the group detection probability set, and Q_{wg}^d is the group detection probability of winning group wg. Line 3-6 calculate marginal detection efficiencies of all candidate sensing groups and sort them in descending order. Line 8-10 determine whether a candidate sensing group can be selected based on the restrictions defined in equation (7). If satisfying the conditions, it will be selected, otherwise the next candidate sensing group will be considered.

Algorithm 2 Reverse Auction and Marginal Detection Efficiency Based Group Selection Algorithm

Initialization:

1. For $CG_l = \{1, \ldots, g, \ldots g_{NG_l}\}$, get: $Bc = \{bc_1, \ldots, bc_g, \ldots bc_{g_{NG_l}}\}$, $Q_G^d = \{Q_1^d, \ldots, Q_g^d, \ldots Q_{g_{NG_l}}^d\}$
2. $WG_l = \emptyset$; $ME = zeros(1, NG_l)$; $Q_{WG_l}^d = 0$

Selection Operation:

3. **for** $g = 1 : |CG_l|$, do
4. $ME(g) = \frac{Q_{WG_l}^d \otimes Q_G^d(CG(g)) - Q_{WG_l}^d}{Bc(CG(g))}$;
5. **end for**
6. Sort CG with descending order of ME;
7. $Q_{WG_l}^d\_cache = Q_{WG_l}^d$; $Q_{WG_l}^f\_cache = Q_{WG_l}^f$;
8. **for** $g = 1 : |CG_l|$, do
   $Q_{WG_l}^d\_cache = Q_{WG_l}^d\_cache \otimes CG_l(g)$;
   $Q_{WG_l}^f\_cache = Q_{WG_l}^f\_cache \otimes CG_l(g)$;
9. **if** $(Q_{WG_l}^d\_cache < \overline{Q}_{th}^d) \& (Q_{WG_l}^f\_cache < \overline{Q}_{th}^f) == 1$
   $CG_l(g) \rightarrow wg$; $wg \rightarrow WG_l$;
   $CG_l = CG_l - WG_l$;
   $ME = zeros(|CG_l|)$; $Q_{WG_l}^d = Q_{WG_l}^d\_cache$;
   break;
10. **else**
    $Q_{WG_l}^d\_cache = Q_{WG_l}^d$; $Q_{WG_l}^f\_cache = Q_{WG_l}^f$;
    end if
    end for
11. Return winning group set WG_l.

Note that the bidding group cost bc_g may be different from the truthful group cost c_g because group members are selfish social and want to obtain more payment from the requestor by reporting a higher cost. However, untruthful group costs will incur a big loss to the benefit of the requestor due to a higher total payment may be expended. Thus it's necessary to design a truthful payment calculation mechanism where any sensing group cannot obtain more payment by biding a higher group cost and consequently the requestor's utility can be guaranteed.

C. TRUTHFUL PAYMENT MECHANISM

In this part we design a requestor-centric payment mechanism where the requestor plays a dominant role in determining how much each winning group will be paid. And then the members within a winning group will share the group reward evenly. Particularly, in our proposed truthful payment mechanism, the payment to a winning group $wg, \forall wg \in WG_l$, by requestor

l is defined as:

$$r_{wg} = (Q^d_{wg}/De_{LG^1_l}) \cdot (1 + \frac{\Delta Q^d_{WG_l}(wg)}{bc_{wg}}) \tag{21}$$

where $\Delta Q^d_{WG_l}(wg)$ is the increment of global detection probability due to winning group wg:

$$\Delta Q^d_{WG_l}(wg) = Q^d_{WG_l} - Q^d_{WG_l \setminus wg} \tag{22}$$

$De_{LG^1_l}$ is detection efficiency of the first group in losing group set LG^1_l:

$$De_{LG^1_l} = \frac{Q^d_{LG^1_l}}{bc^1_{LGl}} \tag{23}$$

Namely, compared with other losing groups, the group LG^1_l has a marginal detection probability ranked only behind the last winning group in WG_l. And bc_{wg} is the bidding group cost of wg. Consequently, based on the novel k-anonymity grouping rule, the winning group selection algorithm and the proposed payment mechanism in equation (21), the optimization problem constructed in equation (7) can be effectively solved.

In a word, out of privacy preservation, the requestor l will firstly allow all his sensing helpers to form a certain number of candidate sensing groups based on both social network and the location proximity. Then he will select an optimal winning group subset WG_l to achieve a target global detection probability with minimal total payment based on a reverse auction mechanism consisting of a marginal detection efficiency based winner selection algorithm and a truthful payment algorithm. As we can see, in our proposed incentive mechanism, not only monetary incentive but also privacy-aware incentive is comprehensively considered to provide a double-motivation for each sensing helper. And consequently, a requestor l can obtain more opportunities to select better winning sensing helpers and meanwhile each winning helper wj in a winning group wg can obtain a satisfied profit to compensate both its sensing cost c^s_{wj} and the privacy leak cost c^{py}_{wj}.

D. PROOF OF ECONOMIC PROPERTIES

A successful auction mechanism needs to satisfy the following favored economic properties: individual rationality, computational efficiency and truthfulness. Thus in order to declare the rationality and the effectiveness of our proposed incentive mechanism, we analyze and prove the three properties respectively in details as follows.

Definition 1 (Individual Rationality): An auction mechanism is individual rational if each winning group or winning helper can obtain a nonnegative utility by participating in the crowdsourced spectrum sensing and reporting truthful cost.

Lemma 1: The proposed reverse auction based incentive mechanism is individual rational.

Proof: Firstly, we analyze the individual rationality of a winning group wg whose utility is defined as follows:

$$u_{wg} = r_{wg} - c_{wg} \tag{24}$$

Due to the fact that requestor l selects winning group according to equation (18), thus the marginal detection efficiency of winning group wg is larger than the losing group LG^1_l:

$$ME_{wg} > ME_{LG^1_l} \tag{25}$$

Namely, $\frac{Q^d_{wg}}{bc_{wg}} > \frac{Q^d_{LG^1_l}}{bc_{LG^1_l}}$, hence we can get

$$Q^d_{wg}/\frac{Q^d_{LG^1_l}}{bc_{LG^1_l}} > bc_{wg} \tag{26}$$

According to equation (22), we obtain

$$\frac{\Delta Q^d_{WG_l}(wg)}{bc_{wg}} > 0 \tag{27}$$

Consequently, we get

$$r_{wg} = (Q^d_{wg}/\frac{Q^d_{LG^1_l}}{bc_{LG^1_l}}) \cdot (1 + \frac{\Delta Q^d_{WG_l}(wg)}{bc_{wg}}) > bc_{wg} \tag{28}$$

When winning group wg reports its truthful group cost, i.e., $bc_{wg} = c_{wg}$, we can get

$$u_{wg} = r_{wg} - c_{wg} = r_{wg} - bc_{wg} > 0 \tag{29}$$

Namely any winning group can obtain a nonnegative utility.

Next, we analyze the utility of each winning helper j within a winning group wg. According to equation (1), we get the group cost of winning group wg: $c_{wg} = c_{wj,\max} \cdot N_{wg}$. Due to equation (29), we can get

$$\begin{aligned} & r_{wg} > c_{wg} \\ \rightarrow & \frac{r_{wg}}{N_{wg}} > \frac{c_{wg}}{N_{wg}} \\ \rightarrow & \frac{r_{wg}}{N_{wg}} > c_{wj,\max} \\ \rightarrow & \frac{r_{wg}}{N_{wg}} > c_{wj}, \quad \forall wj \in wg \end{aligned} \tag{30}$$

Consequently, according to the equation (9), we can obtain

$$u_{wj} = r_{wj} - c_{wj} = \frac{r_{wg}}{N_{wg}} - c_{wj} > 0 \tag{31}$$

Namely, any winning sensing helper can obtain a nonnegative utility. In a word, our proposed auction based incentive mechanism is individual rational. ■

Definition 2 (Computational Efficiency): An auction mechanism is computationally efficient if it can be completed in polynomial time.

Lemma 2: The reverse auction based incentive mechanism is computationally efficient.

Proof: As we can see, the proposed incentive mechanism contains grouping stage, winning group selection stage and payment calculation stage. For the grouping stage in Algorithm 1, its computation complexity is bounded to $O(m_l)$, where m_l is the number of all sensing helpers of requestor l. While in the winning group selection stage, the *for* loop, i.e., the computation of seeking the largest

marginal detection efficiency group is bounded to $O(NG_l)$, where NG_l is the number of candidate sensing groups. Thus the computation complexity of algorithm 2 is bounded to $O\left(NG_l^2\right)$. As for the payment calculation stage, the computation complexity of finding the first losing group in the set of LG_l is bounded to $O(NG_l)$. Furthermore, due to the m_l is much larger than NG_l, thus we get $O(NG_l) < O(m_l)$ and $O\left(NG_l^2\right) < O\left(m_l^2\right)$.

Consequently, the computation complexity of our proposed incentive mechanism is bounded to

$$O(m_l) + O\left(m_l^2\right) + O(m_l) = O\left(m_l^2\right) \tag{32}$$

Thus our proposed reverse auction based incentive mechanism is computational efficient.

Definition 3 (Truthfulness): An auction mechanism is truthful if each sensing helper cannot obtain more payment by reporting a higher sensing cost.

Lemma 3: The reverse auction based incentive mechanism is truthful.

Proof: Proving the truthfulness of an auction mechanism is equivalent to prove the auction is monotone and provides a threshold payment [19], [29].

Firstly, we show that our proposed reverse auction is monotone. Assuming that a sensing group g is selected as a winning group with its bc_g, and if the group g bids a lower group cost bc'_g, it will bring a higher marginal detection efficiency, i.e., $ME_g(bc'_g) > ME_g(bc_g)$. Thus according to the algorithm 2, group g will still win the auction. On the other side, if a sensing user j within group g report a lower cost c'_j, the group cost will not get higher than before. Hence the both the group g and the user j will still be selected in the auction process. Consequently, the reverse auction is monotone.

Next, we prove the threshold payment in our proposed reverse auction mechanism. For a sensing group g, when it claims a higher group cost, there will be two cases happen. The first case: if the bc'_g brings group g a lower marginal detection efficiency even than the marginal detection efficiency of first losing group, i.e., $ME_g(bc'_g) < ME_{LG_l^1}$, group g will lose the auction. The second case: if $ME_g(bc'_g) \geq ME_{LG_l^1}$, the payment to group g will remain the same as before. Thus, the payment to group g, $\forall g \in CG_l$ is a threshold one.

As for a sensing helper j within group g, if it claims a higher cost but still no more than the maximal individual cost in the group, i.e., $c'_j \leq c_{j,\max}$, the group cost will not change and hence the group g will still be selected in auction. Consequently, according to the proposed payment mechanism and equation (10), both the payment to group g and helper $j \in g$ will remain the same. On the contrary, if the helper j claims a higher cost than $c_{j,\max}$, i.e., $c'_j > c_{j,\max}$, the group cost will be larger. And accordingly, the group g will lose the auction or get a same payment as before, hence the helper $j \in g$ will also lose or obtains the same payment. Thus the payment to helper j, $\forall j \in g$ is still a threshold one. Therefore, the proposed reverse auction mechanism provides threshold payment to both sensing group and individual sensing helper.

In conclusion, our proposed reverse auction based incentive mechanism is truthful. ■

IV. POTENTIAL GAME BASED MULTI-USER SPECTRUM SHARING MECHANISM

When transmitter l discoveries the spectrum being vacant based on the reported detection data of winning group set WG_l, he will transmit his data immediately in this channel. However, there may exist other transmitters who also detect the vacant spectrum and will transmit their data in the same channel during the same transmitting time slot. As a result, inevitable interference may exist among these transmitters and finally incur to a degraded global throughput in current channel. Thus in order to solve this problem, we design a game theory [30] based multi-user transmission mechanism where all transmitters in the set $\mathbf{N} = \{1, 2, \ldots, l, \ldots, n\}$ jointly adjust their transmission powers to minimize mutual interference and eventually achieve a maximal global throughput in current channel. Note that in our proposed multi-user spectrum sharing mechanism, we assume that the communications among transmitters are based on a smart phone ad hoc networks [31] where each transmitter leverages existing hardware and software in his own smartphone to create multi-peer ad hoc networks without relying on wireless access points, cellular carrier networks or traditional network infrastructure. In a word, transmitters' individual devices spontaneously compose an ad hoc network to communicate with each other directly rather than going through a centralized access point.

In section II, we have modeled the global throughput maximizing optimization (GTMO) problem as equation (19). However, according to the *reduction algorithm* [32], [33], the proposed optimization problem can be deduced as the reduction from the typical travelling salesman problem (TSP), which means the finding of its globally optimal solution is *NP*-hard and general optimization methods cannot be directly adopted. Thus in this section, we take advantage of the potential game theory [34] to provide a distributed solution of the problem (19) and obtain the game equilibrium based on an improved differential evolution algorithm.

A. POTENTIAL GAME MODEL

In this part, we construct above GTMO problem as a game model $\Phi = (\mathbf{N}, \mathbf{p}, U_G)$, where $\mathbf{N}$ is the set of players (i.e., the transmitters), $\mathbf{p} = \{p_l, \mathbf{p}_{-l}\}$ is the strategy profile of all players, and $U_G(\mathbf{p}) = \sum_{l \in \mathbf{N}} THR_l(\mathbf{p})$ is the global utility, namely the sum of all players' throughputs.

Generally, in game situation, out of selfishness and rationality, each player l will seek for a best strategy p_l^* to maximize its own utility given others' power strategies, namely

$$p_l^* = \arg\max u_l(p_l, \mathbf{p}_{-,l}) \tag{33}$$

where u_l is the utility of player l. Due to existing mutual interference, the strategy adjustment of player l not only

changes its own utility but also has impact on the utility of its neighbors within the set $B_{l,-}$, thus we define the utility function of each player l as follows:

$$u_l(p_l, \mathbf{p}_{-l}) = THR_l(p_l, \mathbf{p}_{-l}) + \sum_{i \in B_{l,-}} THR_i(p_l, \mathbf{p}_{-l}) \quad (34)$$

where $THR_l(p_l, \mathbf{p}_{-l})$ is the throughput of player l defined in equation (17).

As we can see, the search for p_l^* is a distributed solving process for each individual player. While in our proposed game based multi-user transmission mechanism, the jointly optimization of $\mathbf{p}$ is a complex combinational optimization process. Thus if we can prove that the proposed global throughput optimization game is an exact potential game where the variation in individual utility u_l caused by strategy adjustment of player l is equal to the change in potential function, then we can efficiently solve the problem (19) in a distributed method.

Definition 4 (Exact Potential Game): A game is an exact potential game if there exists an exact potential function $\Psi(p_1, \ldots p_l, \ldots p_n), \forall l \in \mathbf{N}$:

$$u_l(p_l', \mathbf{p}_{-l}) - u_l(p_l, \mathbf{p}_{-l}) = \Psi(p_l', \mathbf{p}_{-l}) - \Psi(p_l, \mathbf{p}_{-l}) \quad (35)$$

Lemma 4: The proposed GTMO game Φ is an exact potential game.

Proof: The following proof is inspired by the idea in [35].

(1) Firstly, we construct a potential function:

$$\Psi(p_l, \mathbf{p}_{-l}) = \sum_{l \in \mathbf{N}} THR_l(p_l, \mathbf{p}_{-l}) \quad (36)$$

As a result of $\mathbf{N} = \{l\} \cup C_l \cup NC_l$, the equation (35) can be rewritten as

$$\begin{aligned} \Psi(p_l, \mathbf{p}_{-l}) &= \Psi(p_l, \mathbf{p}_{C_l}, \mathbf{p}_{NC_l}) \\ &= THR_l(p_l, \mathbf{p}_{-,l}) + \sum_{i \in C_l} THR_i(p_l, \mathbf{p}_{-,l}) \\ &\quad + \sum_{i \in NC_l} THR_i(p_l, \mathbf{p}_{-,l}) \end{aligned} \quad (37)$$

where $\mathbf{p}_{C_l} = \{p_i, \forall i \in C_l\}$ is the strategy profile of players within the correlation set C_l and $\mathbf{p}_{NC_l} = \{p_i, \forall i \in NC_l\}$ is the strategy profile of players within the non-correlation set NC_l.

Furthermore, due to $C_l = B_{l,-} \cup B_{-,l}$, equation (37) also can be extended as

$$\begin{aligned} \Psi(p_l, \mathbf{p}_{-l}) &= \Psi(p_l, \mathbf{p}_{B_{l,-}}, \mathbf{p}_{B_{-,l}}, \mathbf{p}_{NC_l}) \\ &= THR_l(p_l, \mathbf{p}_{-,l}) + \sum_{i \in B_{l,-}} THR_i(p_l, \mathbf{p}_{-,l}) \\ &\quad + \sum_{i \in B_{-,l}} THR_i(p_l, \mathbf{p}_{-,l}) + \sum_{i \in NC_l} THR_i(p_l, \mathbf{p}_{-,l}) \end{aligned} \quad (38)$$

When any user l within $\mathbf{N}$ adjusts its power strategy from p_l to p_l', the corresponding change in the potential function can be shown as :

$$\begin{aligned} &\Psi(p_l', \mathbf{p}_{-,l}) - \Psi(p_l, \mathbf{p}_{-,l}) \\ &= \Psi(p_l', \mathbf{p}_{B_{l,-}}, \mathbf{p}_{B_{-,l}}, \mathbf{p}_{NC_l}) - \Psi(p_l, \mathbf{p}_{B_{l,-}}, \mathbf{p}_{B_{-,l}}, \mathbf{p}_{NC_l}) \\ &= \sum_{l \in \mathbf{N}} THR_l(p_l', \mathbf{p}_{-,l}) - \sum_{l \in \mathbf{N}} THR_l(p_l, \mathbf{p}_{-,l}) \\ &= THR_l(p_l', \mathbf{p}_{-,l}) - THR_l(p_l, \mathbf{p}_{-,l}) \\ &\quad + \sum_{i \in B_{l,-}} THR_i(p_l', \mathbf{p}_{-,l}) - \sum_{i \in B_{l,-}} THR_i(p_l, \mathbf{p}_{-,l}) \\ &\quad + \sum_{i \in B_{-,l}} THR_i(p_l', \mathbf{p}_{-,l}) - \sum_{i \in B_{-,l}} THR_i(p_l, \mathbf{p}_{-,l}) \\ &\quad + \sum_{i \in NC_l} THR_i(p_l', \mathbf{p}_{-,l}) - \sum_{i \in NC_l} THR_i(p_l, \mathbf{p}_{-,l}) \end{aligned} \quad (39)$$

For the reason that the strategy adjustment of player l only have impacts on the throughputs of its own and the others who are within its transmission range, i.e., the players within the set $B_{l,-}$, thus we can get

$$\sum_{i \in B_{-,l}} THR_i(p_l', \mathbf{p}_{-,l}) - \sum_{i \in B_{-,l}} THR_i(p_l, \mathbf{p}_{-,l}) = 0 \quad (40)$$

$$\sum_{i \in NC_l} THR_i(p_l', \mathbf{p}_{-,l}) - \sum_{i \in NC_l} THR_i(p_l, \mathbf{p}_{-,l}) = 0 \quad (41)$$

Combining equation (39), (40) and (41), we obtain

$$\begin{aligned} &\Psi(p_l', \mathbf{p}_{-,l}) - \Psi(p_l, \mathbf{p}_{-,l}) \\ &= THR_l(p_l', \mathbf{p}_{-,l}) - THR_l(p_l, \mathbf{p}_{-,l}) \\ &\quad + \sum_{i \in B_{l,-}} THR_i(p_l', \mathbf{p}_{-,l}) - \sum_{i \in B_{l,-}} THR_i(p_l, \mathbf{p}_{-,l}) \end{aligned} \quad (42)$$

(2) Secondly, the strategy adjustment of user l can also bring its utility a variation as follows:

$$\begin{aligned} &u_l(p_l', \mathbf{p}_{-l}) - u_l(p_l, \mathbf{p}_{-l}) \\ &= THR_l(p_l', \mathbf{p}_{-l}) - THR_l(p_l, \mathbf{p}_{-,l}) \\ &\quad + \sum_{i \in B_{l,-}} THR_i(p_l', \mathbf{p}_{-l}) - \sum_{i \in B_{l,-}} THR_i(p_l, \mathbf{p}_{-l}) \end{aligned} \quad (43)$$

As we can see from equation (42) and (43):

$$\Psi(p_l', \mathbf{p}_{-,l}) - \Psi(p_l, \mathbf{p}_{-,l}) = u_l(p_l', \mathbf{p}_{-,l}) - u_l(p_l, \mathbf{p}_{-,l}) \quad (44)$$

which means the variation in individual utility caused by the strategy adjustment of any player is equivalent to the variation in the potential function.

Thus, according to the definition 1, the proposed GTMO game Φ is an exact potential game, where the potential function is $\Psi(\mathbf{p}) = \sum_{l \in \mathbf{N}} THR_l(\mathbf{p}) = U_G(\mathbf{p})$, namely the global utility function. ■

B. ANALYSIS AND SOLUTION OF NASH EQUILIBRIUM

Nash Equilibrium (NE) is a crucial property proving whether a game model is reasonable and can obtain a stable solution. Thus in order to analyze the NE in our proposed GTMO game, we give following definition and lemma.

Definition 5 (Nash Equilibrium): A strategy profile $\mathbf{p}^* = \{p_l^*, \mathbf{p}_{-l}^*\}$ is a pure NE if and only if no player can improve its utility by unilaterally deviating its current strategy, namely

$$u_l(p_l^*, \mathbf{p}_{-l}^*) > u_l(p_l, \mathbf{p}_{-l}^*), \quad \forall l \in \mathbf{N} \tag{45}$$

Lemma 5: The proposed GTMO problem Φ has at least one pure NE.

Proof: According to [35], exact potential game owns an excellent property that is every exact potential game has at least one pure strategy NE solution. Meanwhile, in lemma 4, we have proven our proposed optimization game Φ is an exact potential game, thus Φ has at least one pure NE. And the equilibrium strategy profile $\mathbf{p}^*$ maximizing the utility u_l of player l, $\forall l \in \mathbf{N}$, is also the optimal equilibrium solution to the global utility U_G. ■

Proving the GTMO game being an exact potential game has simplified the combinatorial optimization problem as a distributed NE solving process. Existing equilibrium solving methods mainly based on the typical best response dynamic [36], fictitious play [37] and so on. However, these methods easily trapped in an undesirable equilibrium. Recently, with the rise of machine learning and artificial intelligence, the differential evolution (DE) algorithm [38] has attracted significant attention due to its robustness and strong search capability. Consequently, in this paper, we propose an improved DE algorithm where the differential weight is randomly-adjustable and thus the search capability is increasing. Furthermore, a better solution of Φ can be obtained through stochastic exploration in the search space. The details of the improved DE algorithm are illustrated in Algorithm 3.

As we can see, the proposed improved DE algorithm consists of six parts, namely, the input, initialization, improved mutation operation, crossover operation, greedy selection and Output. Specifically, in the input part, dimension n represents the number of transmitters, population Np represents the search scale of candidate strategies for each transmitter and generation Gm is the total iteration rounds of the whole algorithm. In the initialization part, we firstly define a rational value range for the power strategy of each player l, i.e., $p_l \in [p_{\min}, p_{\max}]$ and then generate an $Np \cdot n$ initial power strategy matrix (i.e., line 4) where each player l has Np initial candidate strategies. Or in another word, we can start the search for optimal solution from the Np initial strategy profiles, which is an effective way to prevent the algorithm running into an unsatisfied local optimization solution.

Then we turn to the improved mutation operation part where F means the differential weight. In this paper, we adopt a dynamic mechanism to obtain the differential weight, namely

$$F = d * rand(0, 1) \tag{46}$$

where d is an constant coefficient. Compared with the existing works with constant differential weight, the adopted improved DE algorithm can randomly update the differential weight, which further brings a dynamic mutation step

Algorithm 3 Improved DE Based NE Solution Algorithm in GTMO Game

Input: Population: Np; Dimension: n; Generation: Gm

Initialization:
1. $gm \leftarrow 1$; $p_{\min} \leftarrow 0$; $p_{\max} \leftarrow P$
2. **for** $i = 1$ **to** Np, **do**
3. **for** $l = 1$ **to** n, **do**
4. $p_{i,l}^{gm} = p_{\min} + rand(0, 1) \cdot (p_{\max} - p_{\min})$;
5. **end**
6. **end**

While $gm \leq Gm$, **do**
Mutation Operation:
7. **for** $i = 1$ to Np, do
8. **for** $j = 1$ to n, do
9. $son = p_{x_1,l}^{gm} + F \cdot (p_{x_2,l}^{gm} - p_{x_3,l}^{gm})$, $\forall x_1, x_2, x_3 \in [1, 2, \ldots, Np]$, $x_1 \neq x_2 \neq x_3$;
10. **if** $0 < son < P$,
11. $t_{i,p}^{gm}\_next\_1 = son$;
12. **else**
13. $p_{i,l}^{gm}\_next\_1 = p_{\min} + rand(0, 1) \cdot (p_{\max} - p_{\min})$;
14. **end if**
15. **end for**
16. **end for**

Crossover Operation:
17. **for** $i = 1$ to Np, do
18. **for** $l = 1$ to n, do
19. **if** $CR \geq rand(0, 1)$ or $l == l_{rand}$,
20. $p_{i,l}^{gm}\_next\_2 = p_{i,l}^{gm}\_next\_1$;
21. **else**
22. $p_{i,l}^{gm}\_next\_2 = p_{i,l}^{gm}$;
23. **end if**
24. **end for**
25. **end for**

Greedy Selection:
26. **for** $i = 1$ **to** Np, **do**
27. **for** $l = 1$ **to** n, **do**
28. **if** $u_l(p_{i,l}^{gm}\_next\_2) > u_l(p_{i,l}^{gm})$
29. $p_{i,l}^{gm} \leftarrow p_{i,l}^{gm}\_next\_2$;
30. **else**
31. $p_{i,l}^{gm} \leftarrow p_{i,l}^{gm}$;
32. **end**
33. **end**
34. compute $U_G(\mathbf{p}_i^{gm})$;
35. **end**
36. $(\mathbf{p}^{gm})^{opt} \leftarrow \arg\max_{\mathbf{p}_i^{gm}} U_G(\mathbf{p})$, $i = 1, 2, \ldots, Np$;
37. $gm \leftarrow gm + 1$;
end while

Output: The best strategy profile $\mathbf{p}^{opt}$
38. Sort $\{U_G((\mathbf{p}^{gm})^{opt}), \forall gm = 1, 2, \ldots, Gm\}$ in descending order and extract all Generation indexes into the vector $\mathbf{best} = \{v | v \in [1, Gm]\}$;
39. $\mathbf{p}^{opt} \leftarrow \mathbf{p}^{\mathbf{best}(1)}$;
40. Obtain the optimal equilibrium strategy profile $\mathbf{p}^{opt}$

(seen in line 9) and consequently can achieve a larger searching scale and a better equilibrium solution. Then based on three randomly selected candidate strategies and the improved mutation method, line 9 generates a new strategy (i.e., the *son*) for each player based on the updated differential weight in equation (46) and lines 10-13 guarantee the *son* within the rational value range. Next in the crossover operation, lines 19-22 update a *next_2* strategy for each player based on the crossover probability *CR* and the another condition $l = l_{rand} = rand(1, \ldots, l, \ldots, n)$, specifically,. Finally, in the stage of greedy selection, for each player, the individual utility respectively based on the *next_2* strategy and initial strategy will be compared in lines 28-34, and the strategy that can obtain a better utility will be selected. Then line 36 obtain the best strategy profile among *Np* options during current iteration *gm*. When all *Gm* iterations finished, the output part will calculate the optimal NE strategy profile $\mathbf{p}^{opt}$ of the GTMO game.

V. SIMULATION RESULTS

In this section, we provide sufficient simulation results to evaluate the performance of our proposed mechanisms and algorithms. Specifically, at first, we illustrate the performance of our proposed privacy preservation mechanism (i.e., the k- anonymity) by comparing with the non-preservation mechanism where all sensing helpers will not form any sensing groups and the requestor will directly select individual helpers based on the marginal detection efficiency defined in equation (20). Furthermore, in contrast with equation (12) – (14), the total cost of any winning helper *wj* in non-preservation mechanism is defined as

$$c_{wj,no-k} = c^{s}_{wj,no-k} + c^{py}_{wj,no-k} = c^{s}_{wj_0} \cdot t_s + a \qquad (47)$$

Secondly, the properties of the proposed reverse auction are further confirmed by simulation results. Then, we analyze the performance of proposed multi-user transmission mechanism where the adopted improved DE algorithm is compared with the typical best response dynamic (BR) and another DE algorithm in recent work to show its advantage in obtaining a better NE of the GTMO problem.

A. SIMULATION SETUP

Our simulation results are achieved in Matlab R2015 environment and the network topology is setup as follows. A crowd number of transmitters and idle mobile sensing users are randomly located in a 3 km × 3 km region, where each transmitter needs to recruit an optimal number of sensing helpers to perform a cooperative spectrum sensing and out of privacy preservation, the candidate sensing helpers will firstly form several sensing groups to hide their individual information. Similar to [22], for each sensing helper *j*, we assume that its sensing cost $\mathbf{T}$ subjects to uniformly distribution ranging from 0 to 1, and the channel gain $h_{j,PU}$ is exponentially distributed with mean value as 0.1. While for each transmitter, the value range of its power strategy is set as $[p_{\min}, p_{\max}] = [0, 200]\ mW$, and the channel gain h_l is also subjected to an exponential distribution with the mean value as 0.2. Moreover, other simulation parameters are listed in Table 2 as follows.

TABLE 2. List of simulation parameters.

Notation	Value	Description
$\mathcal{E}$	0.85	Detection threshold
σ^2	10^{-4}	Noise level
f	6MHz	Sampling frequency
t_s	0.1s	Sensing time slot
E	5MHz	Channel bandwidth
$\overline{Q}^{d}_{th}$	0.9	Expected threshold detection probability
$\overline{Q}^{f}_{th}$	0.15	Expected threshold false alarm probability
n	10	The number of transmitters
NP	100	Population size
d	1.5	The cofficient of differential weight
e	5	The coefficient in global network utility function
CR	0.9	Crossover probability

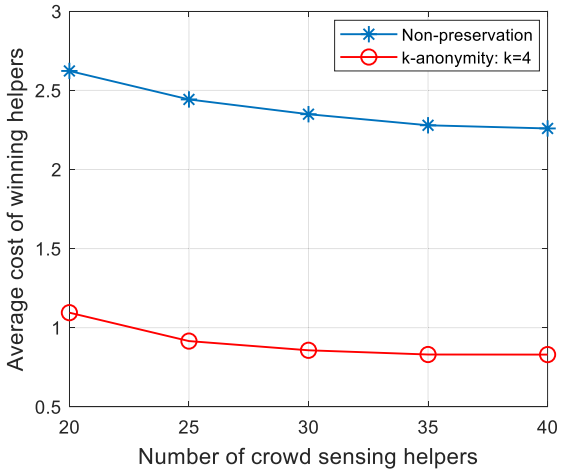

FIGURE 3. Average cost of winning helpers vs. the number of sensing helpers in *k*-anonymity and non-preservation mechanism.

B. PERFORMANCE OF PRIVACY PRESERVATION MECHANISM

In this section, we focus on the performance analysis of our proposed k- anonymity privacy preservation mechanism by comparing with the non-preservation mechanism. Without loss of generality, Fig. 3 - Fig. 7 are achieved by considering one transmitter (or requestor) $l, \forall l \in \mathbf{N}$ and a crowd of sensing helpers H_l he needs to recruit for a cooperative spectrum sensing process.

Specifically, Fig. 3 and Fig. 4 respectively show the average cost of winning helpers and the total payment of requestor versus the number of participating sensing helpers (i.e., m_l) in both k- anonymity and non-preservation mechanism, where $w_{PU} = 200mW$ and $a = 2$.

As we can see from Fig. 3, with the increasing number of participating sensing helpers, the average cost of winning

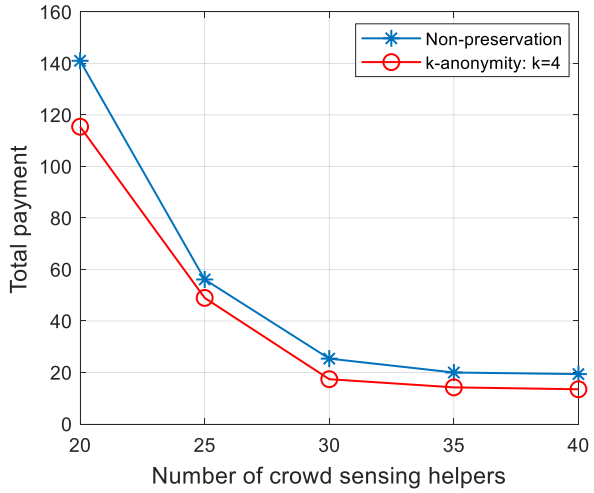

FIGURE 4. Total payment vs. the number of sensing helpers in *k*-anonymity and non-preservation mechanism.

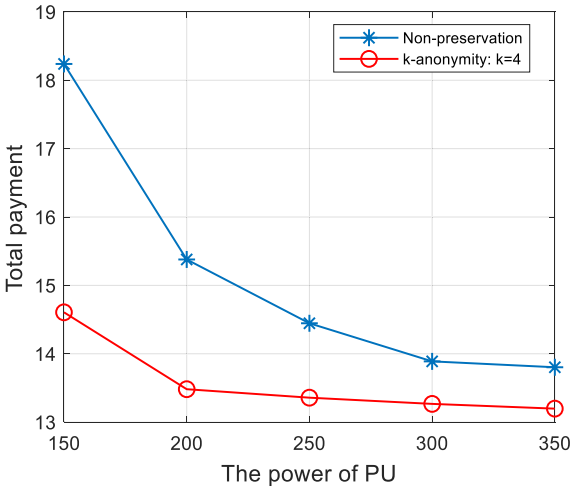

FIGURE 6. Total payment vs. the power of PU in *k*-anonymity and non-preservation mechanism.

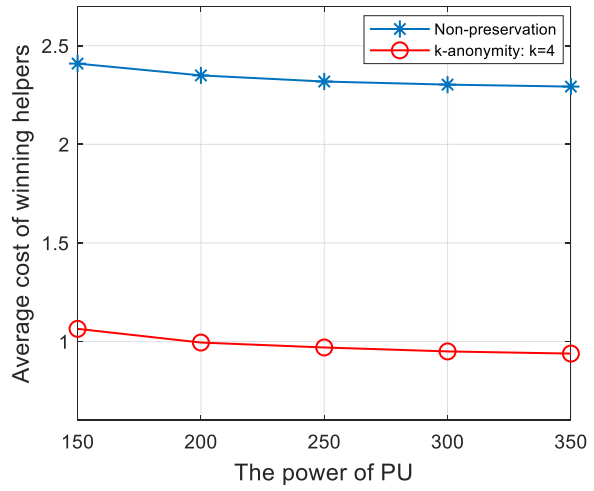

FIGURE 5. Average cost of winning helpers vs. the power of PU in *k*-anonymity and non-preservation mechanism.

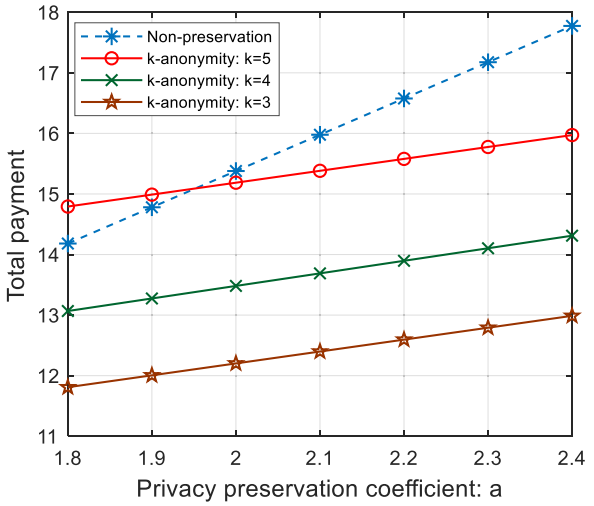

FIGURE 7. Total payment vs. *a* in *k*-anonymity and non-preservation mechanism.

helpers decreases in both two mechanisms. The reason is that the more participating helpers, the more opportunities to form a better sensing group for each helper $\forall j \in H_l$, and consequently the more chance for requestor to select better winning groups (namely, the groups with higher group detection probability and lower group cost) based on the marginal detection efficiency defined in equation (20). While given a same number of sensing helpers, the average cost of winning helpers in our proposed k - anonymity mechanism (where $k = 4$) is evidently lower than and non-preservation mechanism. The result can be explained by equation (12)-(14) and the equation (47). Specifically, in k-anonymity mechanism, the privacy leak cost of each winning helper is lower than in non-preservation mechanism due to the privacy preservation by hiding individual information in a sensing group. Thus the total cost of each winning helper trend to be lower with k - anonymity privacy preservation mechanism.

Fig 4 shows that in both k-anonymity and non-preservation mechanisms, the requestor's total payment decreases with the increasing number of sensing helpers due to the more chances to select better sensing groups. In more details, the requestor can expend a less total payment in our proposed k-anonymity mechanism for the reason that the privacy preservation mechanism decreases both the cost of each winning helper and each sensing group compared with the non-preservation mechanism. Thus when all sensing helpers report their truthful cost, based on the payment mechanism, the requestor can pay a less payment to winning helpers.

Fig 5 and Fig. 6 respectively illustrate the average cost of winning helpers and the total payment versus the transmission power of PU in both k - anonymity and non-preservation mechanisms, where the number of sensing helpers $m_l = 40$ and $a = 2$.

In Fig. 5, we see that the average cost of winning helpers decreases with the increasing transmission power of the PU, which is because that a higher w_{PU} means a higher local detection probability for each sensing helper. Hence given the sensing time slot t_s, the requestor can select a crowd of helpers, who have lower unit sensing cost, to reach the target detection probability $\overline{Q}_{th}^{d}$. Consequently, the average cost of winning helpers gets lower. While given the power of PU, Fig. 5 shows that our proposed privacy preservation mechanism obtains a lower average cost for all winning helpers due to that each wj can get a lower privacy leak cost c_{wj}^{py} by joining a sensing group.

In Fig. 6, the total payment also decreases with the incremental PU's transmission power due to the selection of a better winning group set. Moreover, for the reason that k - anonymity mechanism decreases each group's cost, thus based on our proposed truthful payment mechanism, a lower total payment can be achieved by the sensing requestor, which further proves that our proposed privacy-aware crowdsourced spectrum sensing mechanism can obtain a better solution for the optimization problem in equation (7).

In Fig. 7, we consider the impacts of privacy preservation coefficient a and k on the total payment in two mechanisms, where $w_{PU} = 200mW$, $m_l = 40$. As we can see, the total payment increases with the privacy preservation coefficient in both k- anonymity and non-preservation mechanism, which can be easily explained by the increasing privacy leak cost of each sensing helper in equation (14). Consequently, each group's total cost will also increase and thus the requestor has to expend a higher total payment.

Beyond that, when given the coefficient a, we can get that a higher k gives rise to a higher total payment for the requestor. The reason is that a higher k brings about more sensing helpers in a sensing group where someone who has higher individual cost may be included. Thus according to the equation (1), the group cost will increase and ultimately incur to a higher total payment for the requestor. In more details, we can see that the total payment in non-preservation mechanism is always higher than in $k = 3$ and $k = 4$ anonymity mechanisms, but tends to be lower than $k = 5$ anonymity mechanism when the privacy preservation coefficient a is less than a certain value. This phenomenon illustrates that when each sensing helper pays more attention to its privacy preservation, or in another word, when the privacy leak cost takes a larger fraction in each helper's total cost, our proposed k- anonymity mechanism can obtains a better performance in solving the total payment minimizing optimization problem due to the lower privacy leak cost of each winning helper and the lower group cost.

C. PROPERTIES OF PROPOSED REVERSE AUCTION MECHANISM

In addition to the theoretical proofs about our proposed reverse auction in section III. D, in this part, we also correspondingly provide some credible simulation results to further confirm that our proposed reverse auction based payment mechanism can satisfy the essential economic properties, i.e., the individual rationality and the truthfulness.

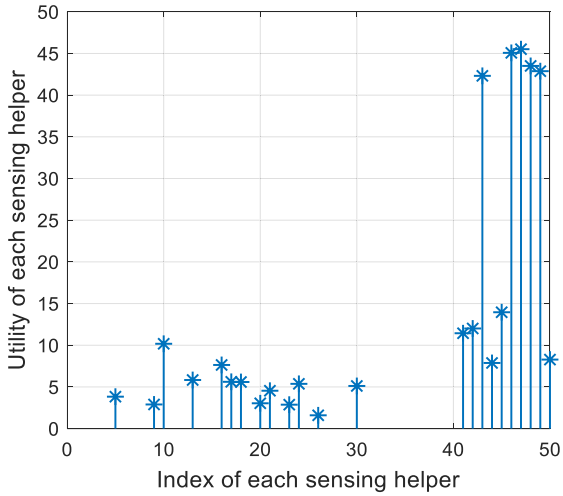

FIGURE 8. The property of individual rationality.

In particular, Fig. 8 proves the individual rational property in our proposed reverse auction mechanism by plotting the utility of each participating sensing helpers, where $w_{PU} = 200mW$, $m_l = 50$, $a = 2$. As we can see, the winning helpers, such as helper 10, helper 30 and helper 50, all can obtain a positive utility by participating and winning in the cooperative spectrum sensing process. While for other candidate sensing helpers, who lose in the winning helper selection part, such as helper 3, helper 31 and helper 35, due to the non-consumption of sensing cost and unnecessity of reporting individual data, they will obtain a zero utility rather than a negative utility, which eventually proves the individual rationality of our proposed reverse auction mechanism.

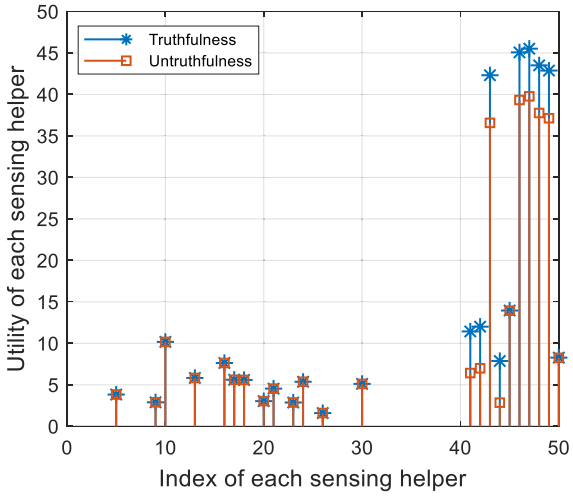

FIGURE 9. The property of truthfulness.

Fig 9 proves the truthfulness in our proposed payment mechanism by comparing with an untruthful mechanism where we assume that a random number of helpers winning

in the truthful mechanism will report higher individual costs. As we can see from the simulation result, when a sensing helper report an untruthful individual cost, such as the helper 41, 42 and 48, he cannot obtain a higher utility than reporting its truthful cost, even he can also win in the winner selection process. Consequently, our proposed payment can achieve the truthful property and eventually offer a higher utility to all winning sensing helpers when they all claim their truthful individual costs.

D. ALGORITHM COMPARISON IN MULTI-USER TRANSMISSION MECHANISM

In this section, we focus on the proposed potential game based multi-user transmission mechanism and specifically analyze the performance of the improved DE algorithm by comparing with the typical best response dynamic algorithm and the DE algorithm proposed in [39].

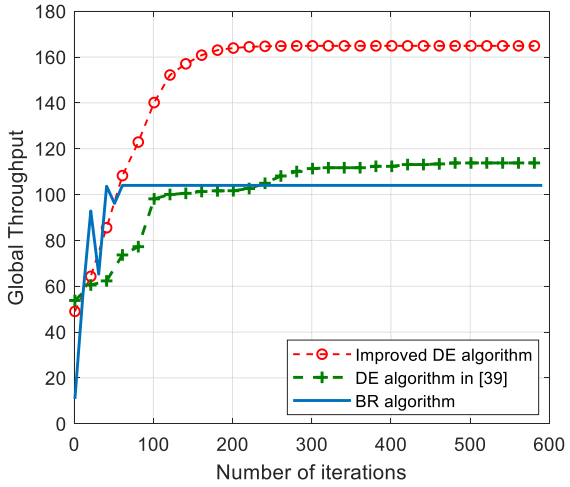

FIGURE 10. Global throughput vs. the number of iterations in different algorithms.

Fig 10 shows the global throughput obtained by our improved DE algorithm verse the number of iterations and simultaneously compared with BR algorithm and the DE algorithm in [39]. As shown in the simulation result, the BR algorithm converges faster but obtains a lowest global throughput compared with our improved DE algorithm and the DE algorithm in [39]. The reason is that the DE algorithm possesses numerous advantages including a strong search capability and the robustness. Furthermore, compared with the DE algorithm in [39], the simulation results show that our proposed improved DE algorithm can achieve a better global throughput, which eventually proves that our improved differential weight is benefit to search more candidate equilibrium solutions and thus obtain a better performance. On the other hand, due to the large search scale, it will take a longer run time for DE algorithm to converge, but in return, a better equilibrium solution, namely a higher global throughput, can be achieved in the GTMO problem. In future works, we will focus on proposing an updated differential evolution algorithm with both better convergence performance and higher global throughput.

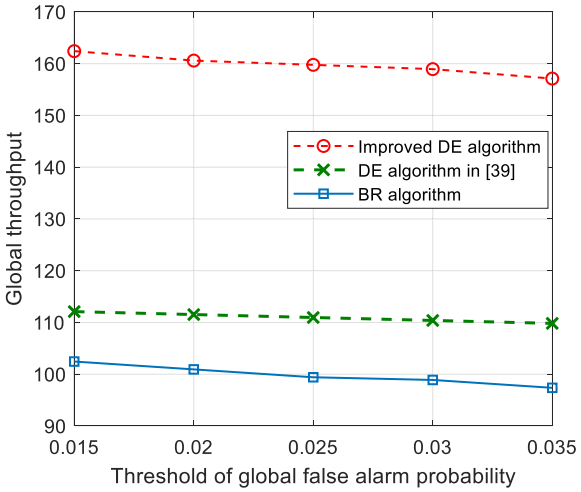

FIGURE 11. Global throughput vs. the threshold of global false alarm probability in different algorithms.

Fig. 11 analyzes the impact of k-anonymity based crowdsourced spectrum sensing on multi-user transmission mechanism where the global throughput in different algorithms versus the threshold of global false probability for each transmitter, i.e., $\overline{Q}_{th}^{f}$, is plotted. As we can see, the higher the $\overline{Q}_{th}^{f}$, the lower the global throughput. This is out of the reason that a high $\overline{Q}_{th}^{f}$ means a high probability that a sensing user may detect a false existence of the PU when actually the spectrum is vacant, and which further indicates a low accuracy about the spectrum status. In more details, the higher $\overline{Q}_{th}^{f}$ may eventually degrade the spectrum access performance for each transmitter and at last the global throughput becomes degraded. The reason for Fig. 11 can also be seen from the equation (17) and (19), where the individual throughput of each transmitter will decrease with the high $\overline{Q}_{th}^{f}$ and thus the global throughput in equation (19) will also be low. Moreover, the simulation results also prove that our proposed improved DE algorithm can achieve a better global performance compared with the other two algorithms. In conclusion, the Fig. 11 shows that a better detection performance, obtained by each transmitter, can give a better guarantee for both individual throughput and the global throughput, which further certifies that it's meaningful to recruit a proper number of sensing helpers participating in the cooperative sensing process.

VI. CONCLUSION

In this paper, we propose a privacy-aware crowdsourced spectrum sensing and multi-user sharing mechanism in dynamic spectrum access networks. To guarantee the detection performance from spatial-domain, in spectrum sensing stage, we take advantage of the mobile crowd sensing to provide a sufficient number of candidate sensing helpers for each transmitter. Considering the individual rationality and sensing consumption, we not only propose a reverse auction based monetary incentive but also a k-anonymity privacy

preservation mechanism to motivate the sensing participations of mobile users. While for each requestor (i.e., each transmitter) in the sensing stage, aiming at achieving a target detection performance with minimal payment, he will select an optimal winning group set based on the marginal detection efficiency ordering. At last, we also give a detailed proof for the essential economic properties of the proposed reverse auction mechanism. Furthermore, in the data transmission stage, we consider a more realistic scenario where based on sensing data from a crowd of sensing helpers, multiple transmitters may discovery an idle spectrum at the same time and will simultaneously transmit their data in current spectrum. Thus in order to achieve a maximum utilization of the spectrum, we propose a potential game based multi-transmission mechanism where all transmitters are regarded as game players and will jointly adjust their transmission power to maximize the global throughput. Then we adopt an improved differential evolution algorithm to obtain a better equilibrium solution in this game. Finally, sufficient simulation results prove the better performance of our proposed mechanism. Considering that spectrum varies dramatically over time, in future works, we will concentrate both spatial and temporal impacts on the dynamic spectrum access networks to achieve a better spectrum utilization.

REFERENCES

[1] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–893, May 2007.

[2] L. P. Belikaidis *et al.*, "Multi-RAT dynamic spectrum access for 5G heterogeneous networks: The SPEED-5G approach," *IEEE Wirel. Commun.*, vol. 24, no. 5, pp. 14–22, Oct. 2017.

[3] M. A. Shattal, A. Wisniewska, A. Al-Fuqaha, B. Khan, and K. Dombrowski, "Evolutionary game theory perspective on dynamic spectrum access etiquette," *IEEE Access*, vol. 6, pp. 13142–13157, 2017.

[4] V. Maglogiannis, D. Naudts, A. Shahid, and I. Moerman, "A Q-learning scheme for fair coexistence between LTE and Wi-Fi in unlicensed spectrum," *IEEE Access*, vol. 6, pp. 27278–27293, 2018.

[5] F. Mohammadian, Z. Pourgharehkhan, A. Taherpour, and T. Khattab, "Optimal collaborative energy harvesting spectrum sensing with limited time resource," in *Proc. IEEE WCNC*, Doha, Qatar, Apr. 2016, pp. 1–7.

[6] W. Zhong, K. Chen, and X. Liu, "Joint optimal energy-efficient cooperative spectrum sensing and transmission in cognitive radio," *China Commun.*, vol. 14, no. 1, pp. 98–110, Jan. 2017.

[7] B. Guo, C. Chen, D. Zhang, A. Chin, and Z. Yu, "Mobile crowd sensing and computing: When participatory sensing meets participatory social media," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 131–137, Feb. 2016.

[8] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 370–380, Oct. 2015.

[9] X. Ying, S. Roy, and R. Poovendran, "Pricing mechanisms for crowdsensed spatial-statistics-based radio mapping," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 2, pp. 242–254, Jun. 2017.

[10] J. Li, Z. Cai, J. Wang, M. Han, and Y. Li, "Truthful incentive mechanisms for geographical position conflicting mobile crowdsensing systems," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 2, pp. 324–334, Jun. 2018.

[11] K. Han, E. A. Graham, D. Vassallo, and D. Estrin, "Enhancing motivation in a mobile participatory sensing project through gaming," in *Proc. PASSAT SocialCom.*, Boston, MA, USA, Oct. 2011, pp. 1443–1448.

[12] J. An, X. Gui, Z. Wang, J. Yang, and X. He, "A crowdsourcing assignment model based on mobile crowd sensing in the Internet of Things," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 358–369, Oct. 2015.

[13] Y. Wang, W. Dai, Q. Jin, and J. Ma, "BciNet: A biased contest-based crowdsourcing incentive mechanism through exploiting social networks," *IEEE Trans. Syst., Man Cybern. -Syst.*, to be published. doi: 10.1109/TSMC.2018.2837165.

[14] L. Jiang, X. Niu, J. Xu, Y. Wang, Y. Wu, and L. Xu, "Time-sensitive and sybil-proof incentive mechanisms for mobile crowdsensing via social network," *IEEE Access*, vol. 6, pp. 48156–48168, 2018.

[15] G. Ding *et al.*, "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014.

[16] B. Gao *et al.*, "Incentivizing spectrum sensing in database-driven dynamic spectrum sharing," in *Proc. IEEE INFOCOM*, San Francisco, CA, USA, Apr. 2016, pp. 1–9.

[17] Y. Hu and R. Zhang, "Secure crowdsourced radio environment map construction," in *Proc. IEEE 25th ICNP*. Toronto, ON, Canada, Oct. 2017, pp. 1–10.

[18] X. Wang, Z. Liu, X. Tian, X. Gan, Y. Guan, and X. Wang, "Incentivizing crowdsensing with location-privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6940–6952, Oct. 2017.

[19] J. Lin, D. Yang, M. Li, J. Xu, and G. Xue, "Frameworks for privacy-preserving mobile crowdsensing incentive mechanisms," *IEEE Trans. Mobile Comput.*, vol. 17, no. 8, pp. 1851–1864, Aug. 2018.

[20] Z. Zhang, S. He, J. Chen, and J. Zhang, "REAP: An efficient incentive mechanism for reconciling aggregation accuracy and individual privacy in crowdsensing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 12, pp. 2995–3007, Dec. 2018.

[21] X. Jin and Y. Zhang, "Privacy-preserving crowdsourced spectrum sensing," *IEEE/ACM Trans. Netw.*, vol. 26, no. 3, pp. 1236–1249, Jun. 2018.

[22] H. Zhang, Y. Nie, J. Cheng, V. C. M. Leung, and A. Nallanathan, "Sensing time optimization and power control for energy efficient cognitive small cell with imperfect hybrid spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 730–743, Feb. 2017.

[23] F. Awin, E. Abdel-Raheem, and M. Ahmadi, "Joint optimal transmission power and sensing time for energy efficient spectrum sensing in cognitive radio system," *IEEE Sensors J.*, vol. 17, no. 2, pp. 369–376, Jan. 2017.

[24] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[25] Y. C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[26] J. Wang, Y. Li, D. Yang, H. Gao, G. Luo, and J. Li, "Achieving effective k-anonymity for query privacy in location-based services," *IEEE Access*, vol. 5, pp. 24580–24592, 2017.

[27] L. Zheng, H. Yue, Z. Li, X. Pan, M. Wu, and F. Yang, "k-anonymity location privacy algorithm based on clustering," *IEEE Access*, vol. 6, pp. 28328–28338, 2018.

[28] K.-H. Han and J.-H. Kim, "Quantum-inspired evolutionary algorithm for a class of combinatorial optimization," *IEEE Trans. Evol. Comput.*, vol. 6, no. 6, pp. 580–593, Dec. 2002.

[29] R. B. Myerson, "Optimal auction design," *Math. Oper. Res. Math. Oper. Res.*, vol. 6, no. 1, pp. 58–73, Feb. 1981.

[30] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197–209, Jan. 2018.

[31] C. K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*, 2rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2002.

[32] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 3rd ed. Cambridge, MA, USA: MIT Press, 2001.

[33] X. Li and Q. Zhu, "Social incentive mechanism based multi-user sensing time optimization in co-operative spectrum sensing with mobile crowd sensing," *Sensers*, vol. 18, no. 1, p. 250, Jan. 2018.

[34] D. Monderer and L. S. Shapley, "Potential games," *Games Econ. Behavior*, vol. 14, no. 1, pp. 124–143, 1996.

[35] J. Zheng, Y. Cai, Y. Liu, Y. Xu, B. Duan, and X. Shen, "Optimal power allocation and user scheduling in multicell networks: Base station cooperation using a game-theoretic approach," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6928–6942, Dec. 2014.

[36] K. Schubert, N. Master, Z. Zhou, and N. Bambos, "Asynchronous best-response dynamics for resource allocation games in cloud computing," in *Proc. ACC*. Seattle, WA, USA, May 2017, pp. 4613–4618.

[37] L. Rose, S. Lasaulce, S. M. Perlaza, and M. Debbah, "Learning equilibria with partial information in decentralized wireless networks," *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 136–142, Aug. 2011.

[38] R. Storn and K. Price, "Differential evolution—A simple and efficient heuristic for global optimization over continuous spaces," *J. Glob. Optim.*, vol. 11, no. 4, pp. 341–359, Dec. 1997.
[39] H. Megherbi and A. C. Megherbi, "Differential evolution based identification of the LuGre friction model in the cart motion of an inverted pendulum system," in *Proc. ICSC*. Batna, Algeria, Jun. 2017, pp. 1–5.

XIAOHUI LI received the B.S. degree in information engineering from Tianjin Normal University, Tianjin, China, in 2014. She is currently pursuing the Ph.D. degree with the Key Wireless Laboratory of Jiangsu Province, School of Telecommunication and Information Engineering, Nanjing University of Posts and Telecommunications. She is also a Visiting Student with the Department of Electrical and Computer Engineering, Western University. Her research interests include mobile crowd sensing, incentive mechanism, dynamic spectrum access, game theory, and machine learning.

QI ZHU received the bachelor's and master's degrees in radio engineering from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 1986 and 1989, respectively, where she is currently a Professor with the School of Telecommunication and Information Engineering. Her research interests include technology of next-generation communication, broadband wireless access, orthogonal frequency-division multiplexing, channel and source coding, and dynamic allocation of radio resources.

XIANBIN WANG (S'98–M'99–SM'06–F'17) received the Ph.D. degree in electrical and computer engineering from the National University of Singapore, in 2001.

From 2002 to 2007, he was a Research Scientist/Senior Research Scientist with the Communications Research Centre Canada. From 2001 to 2002, he was a System Designer with STMicroelectronics, where he was responsible for the system design of DSL and gigabit Ethernet chipsets. He is currently a Professor and the Tier-I Canada Research Chair with the University of Western Ontario, Canada. He has over 300 peer-reviewed journal and conference papers, in addition to 26 granted and pending patents and several standard contributions. His current research interests include 5G technologies, the Internet of Things, communications security, machine learning, and locationing technologies.

Dr. Wang is a Fellow of the Canadian Academy of Engineering and an IEEE Distinguished Lecturer. He has received many awards and recognitions, including the Canada Research Chair, the CRC President's Excellence Award, the Canadian Federal Government Public Service Award, the Ontario Early Researcher Award, and the five IEEE Best Paper Awards. He was involved in many IEEE conferences, including the GLOBECOM, ICC, VTC, PIMRC, WCNC, and CWIT, in different roles, such as the Symposium Chair, a Tutorial Instructor, the Track Chair, the Session Chair, and the TPC Co-Chair. He was also an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, from 2007 to 2011, and the IEEE WIRELESS COMMUNICATIONS LETTERS, from 2011 to 2016. He currently serves as an Editor/Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON BROADCASTING, and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.