Xu *et al. EURASIP Journal on Advances in Signal Processing* (2021) 2021:42
https://doi.org/10.1186/s13634-021-00764-0

EURASIP Journal on Advances in Signal Processing

RESEARCH Open Access

Hierarchical coordinated anti-jamming channel access in clustering networks: a multi-leader multi-follower Stackelberg game approach

Yifan Xu, Jin Chen, Zhibin Feng*, Kailing Yao, Guoxin Li, Fei Song and Gui Fang

*Correspondence:
fengzb1995@163.com
College of Communications Engineering, Army Engineering University of PLA, Nanjing, China

Abstract

This paper mainly investigates the multi-user coordinated anti-jamming problem in clustering communication networks. In such kinds of networks, there exist multiple clusters and multiple users who communicate with their receivers simultaneously. Besides, a malicious jammer persistently attacks channels with wide-band and dynamic changing jamming signals. To cope with these challenges brought by the large-scale clustering network and the dynamic wide-band jamming, a hierarchical coordinated anti-jamming approach is proposed, and a multi-leader multi-follower Stackelberg game is introduced to model the anti-jamming problem. In detail, cluster heads act as leaders, and select available frequency bands to avoid jamming attacks, while users in each cluster act as followers and select corresponding channels distributedly and independently. Moreover, it is proved that there exist multiple Stackelberg equilibriums (SEs) in the proposed game. To obtain SEs, a hierarchical coordinated anti-jamming channel access (HCACA) algorithm is designed. Simulation results illustrate that the proposed approach is effective to cope with the dynamic wide-band jamming attacks. Furthermore, it is also depicted that the proposed approach outperforms the distributed anti-jamming comparative approach in terms of convergence speed.

Keywords: Multi-user coordinated anti-jamming, Stackelberg game, Channel access, Dynamic wide-band jamming

1 Introduction

With the development of wireless communication technologies, the number of wireless communication devices increases explosively, causing severe shortage of spectrum resources. Thus, how to coordinate the internal interference is a vital problem that remains to be solved. In addition, due to the advance of the software-defined radio, it is convenient for malicious users (e.g., malicious jammer) to carry out jamming attacks with low-cost and wide-band noise signals; hence, there exists more serious security threaten for communication devices. In a word, it is an important issue to "coordinate the internal interference" and "resist external malicious attacks" simultaneously in wireless communication networks [1–4].

Focusing on the internal coordination and external confrontation problem for effective spectrum resource utilization, game theory [5–14] is a feasible tool to model and analysis the internal and external competitive or cooperative relationships among different decision-makers (i.e., users or malicious jammer). For example, as for internal coordination, authors in [6] reviewed the decision-theoretic solutions for channel access strategies in the opportunistic spectrum access system and presented some effective game models with respect to internal interference avoidance. Besides, authors in [7] reviewed the applications of repeated games in wireless networks, while authors in [8] formulated users' competition for channel access using a non-cooperative game and proved that the proposed game model is an ordinal potential game where there exists at least one pure strategy Nash equilibrium (NE).

While considering the existence of malicious jamming attacks, the Stackelberg game [15–27] is a suitable game model to formulate the competitive interactions between the user-side and the jammer-side as it can well depict the sequential decision-making relationship between two countermeasure sides. For example, Yang et al. formulated the anti-jamming power control problem using the Stackelberg game [15, 16]. In detail, the user was the leader, and the smart jammer acted as the follower of the game. Besides, the utility functions of the user and the jammer were designed respectively. Authors in [17] considered the anti-jamming power control problem with observation error and derived the Stackelberg equilibrium (SE) of the proposed Stackelberg game. In addition, the authors in [18] formulated the competition between one user and one jamming as a Bayesian Stackelberg game and took the incomplete information into consideration. In [19], the authors investigated the discrete anti-jamming power control problem, and solved the problem using the Stackelberg game and Q-learning algorithm. Considering the multi-user anti-jamming scenario, in [20], a one-leader multi-follower Bayesian Stackelberg game was formulated, and the influence of observation error as well as mobility of unmanned aerial vehicles (UAVs) were investigated. Moreover, authors in [21] investigated the communication confrontation scenario, and modeled the interactions in the confrontation scenario as a Stackelberg game, with each player seeking for maximizing their utility respectively.

However, there exist some main challenges to extend the above game approaches to the multi-user coordinated channel access scenario in the clustering networks with dynamic wide-band jamming attacks. (i) The increase of network scale causes more severe internal conflicts, thus it is important to coordinate the co-channel interference as well as to reduce the convergence time and complexity of the channel access algorithm. (ii) Considering the existence of the dynamic wide-band attacker, it is harder for users to adapt to the dynamic change of the jamming attack and to avoid the wide-band jamming signals which take up more spectrum resources than the single tone jamming signals.

To solve these challenges, and to fully take advantage of the clustering network, a multi-leader multi-follower Stackelberg game is formulated to model the competitive interactions between cluster heads and cluster users. Moreover, to accommodate the dynamic changing of the jamming attacks, the idea of jamming utilization is also introduced. To sum up, the main contributions of this paper are as follows:

- The malicious wide-band jamming signals are "utilized" by cluster heads as coordination signals [28] to guide channel access of users, which means for different

sensed jamming signals, different anti-jamming channel access strategies are adopted by users. The application of coordination signals helps users to adapt to the dynamic changing of jamming attacks.

- A multi-leader multi-follower Stackelberg game is formulated, where cluster heads act as leaders, and select available frequency bands to avoid jamming attacks. While users in each cluster act as followers, and select corresponding channels distributedly and independently.
- The proposed Stackelberg game is decomposed into multi-leader sub-game from the coarse granularity and the multi-follower sub-game from the fine granularity. It is proved that the proposed game has at least one SE for each jamming attack.
- To obtain SEs, a hierarchical coordinated anti-jamming channel access (HCACA) algorithm is designed. In addition, simulation results illustrate that the proposed approach is effective to cope with the dynamic wide-band jamming attacks, and it accelerates the convergence of the clustering network compared with the distributed learning scheme.

Note that some existing works investigated the anti-jamming problem using game-theoretic framework [20, 29]. The main differences are summarized as follows: as mentioned in Section 1, the authors in [20]proposed a one-leader multi-follower Bayesian Stackelberg game, and the closed-form of the SE was derived. However, work [20] is not suitable for multi-user scenarios with a large scale, and the proposed approach can not adapt to the dynamic changing characteristic of jamming attacks. Besides, in [29], the authors investigated the distributed coordinated anti-jamming scenario. However, the proposed approach may not be well-adapted to the wide-band jamming in the clustering network. Thus, different from these two works, we fully take advantage of the clustering network in this work, and then propose a hierarchical coordinated anti-jamming channel access approach that is effective with the property of fast convergence.

The rest of this paper is organized as follows. In Section 2, methods are introduced briefly. In Section 3, the system model and problem formulation are presented. In Section 4, the multi-leader multi-follower Stackelberg game for hierarchical coordinated anti-jamming channel access is formulated. While in Section 5, the hierarchical coordinated anti-jamming channel access algorithm is proposed. In Section 6, simulation results and discussions are illustrated. Finally, the conclusion is made in Section 7.

2 Methods

The aim of this study is to solve the multi-user coordinated anti-jamming channel access problem in clustering communication networks. In detail, we propose a hierarchical coordinated anti-jamming approach, and formulate the anti-jamming problem as a multi-leader multi-follower Stackelberg game. Besides, we prove that there exist multiple Stackelberg Equilibriums (SEs) in the proposed game, and we then design a hierarchical coordinated anti-jamming channel access (HCACA) algorithm to obtain NEs of the game.

The paper presents a “game & learning” structure, where the proposed game is used to model the interactions among different decision-makers, and the proposed learning algorithm is to find the optimal or nearly optimal solutions of the game model. The theoretical analysis is supported by the experimental evaluation with the randomly generated cluster-

ing network under different dynamic wide-band jamming patterns, while the simulations have been carried out with Matlab R2019a.

3 System model and problem formulation

3.1 System model

In this paper, we consider a multi-user clustering network that is under the attack of a malicious jammer. As shown in Fig. 1, the network is divided into H clusters according to the geographical location of communication devices [30], and the cluster set is $\mathcal{H}=\{1,...,h,...,H\}$. Besides, the neighbor set of cluster h is denoted as $\mathcal{J}_h$. In each cluster, there exist multiple transmitter-receiver pairs, and each transmitter-receiver pair is assumed to be one user. Denote M_h as the number of users in cluster h, and the user set is $\mathcal{M}_h$. In cluster h, the kth user is denoted as $m_{h,k}$, thus we have $m_{h,k} \in \mathcal{M}_h$. There exist A orthogonal channels for users to access, and the channel set is $\mathcal{A}$. To disturb the legitimate transmissions of users, a malicious jammer incessantly sends high-power noise signals to multiple channels.

In each cluster, there exists a cluster head who can exchange information with cluster users. For example, each cluster head can send available frequency band information to its governed users. After obtaining such frequency information, cluster users are able to select their transmission channels distributedly. Denote the transmission channel of user k in cluster h as $a_{h,k}$, and the transmission throughput of this user is expressed as follows:

$$R_{h,k} = \Delta\left(a_{h,k}, a_{-(h,k)}, A_j\right) B_{a_{h,k}} \log_2\left(1 + \frac{P_{h,k} G_{h,k}}{N_{a_{h,k}}}\right), \tag{1}$$

where $B_{a_{h,k}}$ is the channel bandwidth, $P_{h,k}$ is the transmission power of the kth user in cluster h, and $G_{h,k}$ is the channel gain of the transmission link. Assume that wireless

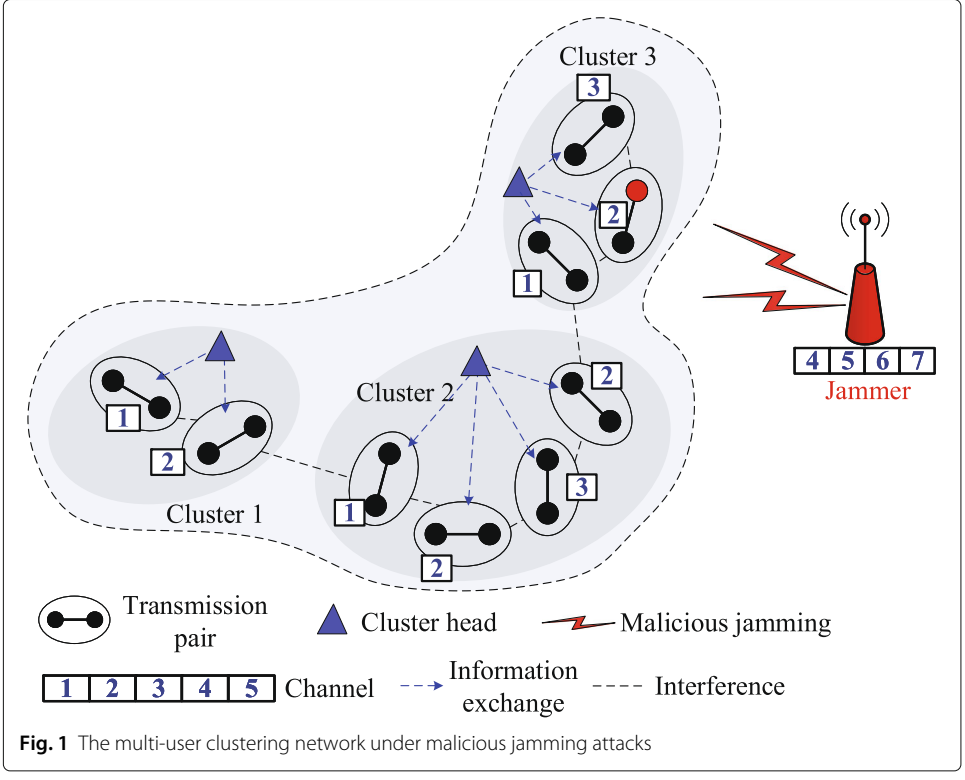

Fig. 1 The multi-user clustering network under malicious jamming attacks

communication channels undergo block fading, and the Rayleigh fading channel model is considered [31]. Thus, $G_{h,k} = d_{h,k}^{-\alpha}\varepsilon_{h,k}$, where $d_{h,k}$ denotes the transmission distance, α is the path-loss factor, and $\varepsilon_{h,k}$ is the instantaneous random component. Besides, $N_{a_{h,k}}$ is the noise power of the channel. In this paper, users adopt multiple access technique that is based on multi-channel slotted ALOHA, and only one transmission is allowed in a slot. To show the influence of the intra-cluster interference, inter-cluster interference and external malicious jamming, a cumulative jamming-interference indicator function $\Delta\left(a_{h,k}, a_{-(h,k)}, A_j\right)$ is designed [32], where $a_{-(h,k)}$ denotes the channel access strategy combination of all users except the kth user in cluster h, and A_j is the jamming channel combination of the malicious jammer. In detail, $\Delta\left(a_{h,k}, a_{-(h,k)}, A_j\right)$ is expressed as follows:

$$\begin{aligned}\Delta\left(a_{h,k}, a_{-(h,k)}, A_j\right) = \\ \underbrace{\left[1-\delta\left(a_{h,k}, A_j\right)\right]}_{\text{External malicious jamming}} \underbrace{\prod_{i\in\mathcal{M}_h\backslash k}\left[1-\delta\left(a_{h,k}, a_{h,i}\right)\right]}_{\text{Intra-interference}} \underbrace{\prod_{g\in\mathcal{J}_h}\prod_{i\in\mathcal{M}_g}\left[1-\delta\left(a_{h,k}, a_{g,i}\right)\right]}_{\text{Inter-interference}},\end{aligned} \tag{2}$$

where $\mathcal{M}_h\backslash k$ denotes all users in cluster h except user k, $a_{h,i}$ is the channel access strategy of user i in the cluster, while $a_{g,i}$ is the channel access strategy of user i in the neighboring cluster g. Note that there exist three indicator functions $\delta\left(a_{h,k}, a_{h,i}\right)$, $\delta\left(a_{h,k}, a_{g,i}\right)$ and $\delta\left(a_{h,k}, A_j\right)$, which show the intra-cluster interference, the inter-cluster interference and the external malicious jamming respectively. Besides, these indicator functions can be denoted as follows:

$$\delta\left(a_{h,k}, a_y\right) = \begin{cases} 1, a_{h,k} = a_y \& P_y d_{y\to h,k}^{-\alpha} > \tau_{\text{thres}}, \\ 0, \text{otherwise}. \end{cases} \tag{3}$$

where $P_y d_{y\to h,k}^{-\alpha} > \tau_{\text{threshold}}$ represents that the received interference/jamming signal power from user/jammer y is higher than the threshold $\tau_{\text{threshold}}$. The above indicator function illustrates that if the channel access strategies of users are conflicting, they will suffer from co-channel interference when the interference threshold is reached. While if the channel access strategy of one user is overlapped with the attack strategy of the malicious jammer, this user will suffer from malicious jamming as the jammer will send high-power noise signals to those attacking channels. Note that the jammer is able to carry out wide-band jamming attacks, the above relationship turns to $a_{h,k} \in A_j$ for the wide-band jamming case.

3.2 Problem formulation

Denote the channel set obtained by the cluster h as $\mathcal{A}_h$, thus we have $a_{h,k} \in \mathcal{A}_h$. Besides, the optimization objective of the clustering network is:

$$\begin{aligned}\mathbf{P}_1: \left(\mathbf{a}_1^*, \cdots \mathbf{a}_H^*\right) = \arg\max \sum_{h\in\mathcal{H}}\sum_{k\in\mathcal{M}_h} R_{h,k} \\ s.t. \left|A_j\right| \le |\mathcal{A}|, \\ \left|a_{h,k}\right| \le 1, \forall h \in \mathcal{H}, \forall m_{h,k} \in \mathcal{M}_h.\end{aligned} \tag{4}$$

where $\mathbf{a}_h^* = \left(a_{h,1}^*, ..., a_{h,\mathcal{M}_h}^*\right), \forall h \in \mathcal{H}$ is all users' channel access strategies in the cluster h. The above optimization objective indicates that each user is willing to find a optimal channel access strategy to maximize the sum of the throughput of the clustering network. The first constraint condition limits the range of jamming channels, while the second

constraint means that each user either selects one channel or keeps silent at each time slot.

However, there exist some challenges to solve the above optimization objective. (i) The optimization objective is a non-convex problem, which is difficult to be solved directly in distributed clustering networks. (ii) Due to the dynamic and wide-band characteristics of malicious jamming, cluster users should coordinate internal interference and avoid external jamming attacks. (iii) With the increase of the network scale, the computation complexity increases correspondingly, and thus, a low-complexity channel access approach is preferred to enhance the convergence speed of the network. To cope with these three challenges, the idea of "game and learning" is introduced, in which a multi-leader multi-follower Stackelberg game is formulated to analyze the relationship among users, and a hierarchical coordinated anti-jamming channel access algorithm is designed to obtain the game equilibriums.

4 Multi-leader multi-follower Stackelberg game for hierarchical coordinated anti-jamming channel access

4.1 Stackelberg game formulation

To solve the hierarchical coordinated anti-jamming channel access problem in the clustering network, a multi-leader multi-follower Stackelberg game is formulated firstly, where cluster heads act as multiple leaders of the game, while cluster members are followers. Besides, the proposed game model can be decomposed into multi-leader sub-game and multi-follower sub-game, as shown in Fig. 2.

Considering the influence of the malicious, wide-band and dynamic jamming attacks, each cluster competes with the jammer to obtain available spectrum bands for its cluster members. Due to the dynamic characteristic of the jammer, the band selection strategies of each cluster need to be adjusted to adapt to the changing of the attacking strategies. After avoiding the malicious jamming bands, each cluster sends available band information to its cluster members. Then, users in the cluster access these available channels

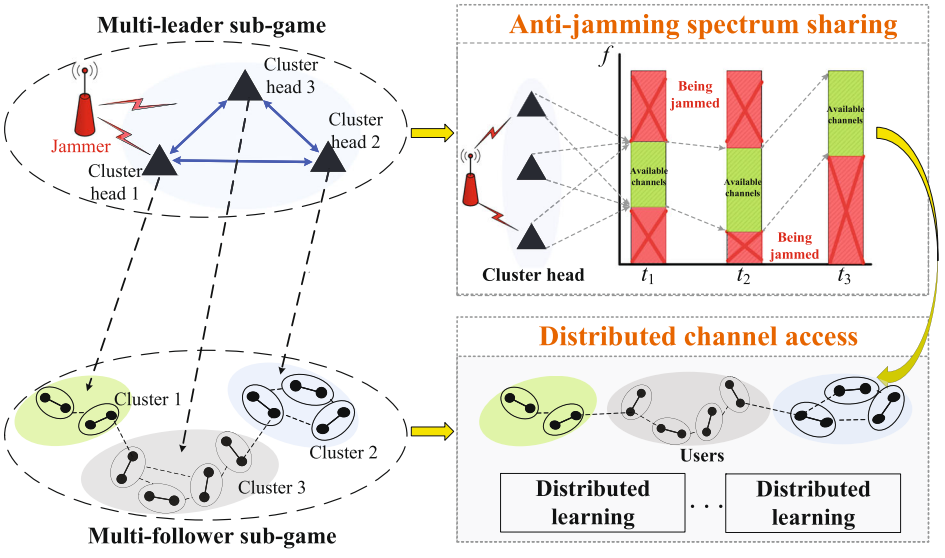

Fig. 2 The structure of multi-leader multi-follower Stackelberg game

distributedly to coordinate the intra-cluster and inter-cluster conflicts. Mathematically, the game model is expressed as follows:

$$\mathcal{G} = \left\{ \mathcal{H}, \{\mathcal{M}_h\}_{h\in\mathcal{H}}, \mathcal{A}, \mathcal{J}, \{\mathcal{A}_h\}_{h\in\mathcal{H}}, \{U_h\}_{h\in\mathcal{H}}, \left\{u_{h,k}\right\}_{h\in\mathcal{H},k\in\mathcal{M}_h}, \mathcal{A}_j \right\}, \tag{5}$$

where $\mathcal{H}$ is the cluster set, $\{\mathcal{M}_h\}_{h\in\mathcal{H}}$ is the user set of each cluster, and $\mathcal{J}$ represents the jammer. $\mathcal{A}$ is the channel set of the clustering network, $\{\mathcal{A}_h\}_{h\in\mathcal{H}}$ is the channel set of each cluster $h \in \mathcal{H}$, and U_h is the utility function of cluster head h. $u_{h,k}$ is the utility function of the user k in the cluster h, which is the same as the throughput $R_{h,k}$ shown in Eq. 1. In addition, $\mathcal{A}_j$ is the attack strategy set of the wide-band jammer.

After the Stackelberg game formulation, the definition of Stackelberg equilibrium (SE) is given, which is shown as follows:

Definition 1 *In the proposed multi-leader multi-follower Stackelberg game, SE delivers the optimal strategy combination of cluster heads and users for each jamming strategy $A_j \in \mathcal{A}_j$. For multiple leaders, there exists strategy combination $\left(A_1^*, \cdots A_H^*\right)$, which maximizes the cumulative utility of the cluster heads. While for multiple followers, strategy combination $\left\{\left(a_{1,1}^*, \cdots a_{1,\mathcal{M}_1}^*\right) \ldots \left(a_{H,1}^*, \cdots a_{H,\mathcal{M}_H}^*\right)\right\}$ is the best-response strategy combination with respect to leaders' strategies [33]. Here, strategy combination $\left\{\left(A_1^*, \cdots A_H^*\right), \left(a_{1,1}^*, \cdots a_{1,M_1}^*\right) \ldots \left(a_{H,1}^*, \cdots a_{H,M_H}^*\right)\right\}$ is the SE of the game, which satisfies the following conditions:*

$$\begin{cases} U_h\left(A_h^*, A_{-h}^*, a_{1,1}^*, ..., a_{H,\mathcal{M}_H}^*\right) \geq U_h\left(A_h, A_{-h}^*, a_{1,1}^*, ..., a_{H,\mathcal{M}_H}^*\right), \forall h \in \mathcal{H}, \\ u_{h,k}\left(a_{h,k}^*, a_{-(h,k)}^*, A_h^*, A_{-h}^*\right) \geq u_{h,k}\left(a_{h,k}, a_{-(h,k)}^*, A_h^*, A_{-h}^*\right), \forall h \in \mathcal{H}, k \in \mathcal{M}_h. \end{cases} \tag{6}$$

In Eq. 6, A_{-h}^* denotes all the cluster heads' optimal strategy combination except cluster head h, and $a_{-(h,k)}^*$ is all users' best-response strategy combination except user k in cluster h.

According to the hierarchical characteristic of the multi-leader multi-follower Stackelberg game, the optimization objective $\mathbf{P}_1$ is rewritten as:

$$\begin{cases} For\ h = 1, ..., H \\ \max\limits_{A_h} U_h\left(A_h, A_{-h}, A_j\right), h \in \mathcal{H}, A_h \in \mathcal{A}_h \\ \text{The best response solution}: a_{1,1}^*, ..., a_{H,\mathcal{M}_H}^* \\ \quad \begin{cases} \max\limits_{a_{h,k}} u_{h,k}\left(a_{h,k}, a_{-(h,k)}\right), \\ a_{h,k} \in A_h \end{cases} \end{cases} \tag{7}$$

Note that there are multiple coupling relationships in the clustering network, and there also exist competitive relationships between different clusters and the malicious jammer, thus the above game formulation is hard to be solved directly using traditional optimization approaches. In this paper, the game is decomposed into two sub-games from two different granularities, that is, the multi-leader(cluster head) sub-game anti-jamming spectrum sharing from the coarse granularity, and the multi-follower (cluster member) distributed channel access from the fine granularity.

4.2 Multi-leader sub-game from the coarse granularity

The objective of the multi-leader sub-game is to analyze and model the competitive interactions between different cluster heads and the jammer. Generally, this sub-game is formulated as:

$$\mathcal{G}_{\mathrm{ML}} = \left\{\mathcal{H}, \{\mathrm{CH}_h\}_{h\in\mathcal{H}}, \mathcal{A}, \mathcal{J}, \{\mathcal{A}_h\}_{h\in\mathcal{H}}, \{U_h\}_{h\in\mathcal{H}}, \mathcal{A}_j\right\}, \tag{8}$$

where CH_h is the cluster head of the cluster h, $A_h \subseteq \mathcal{A}_h$ is one of the band selection strategy of the cluster h, $A_j \subseteq \mathcal{A}_j$ is one of the jamming strategy, and U_h is the utility function of corresponding cluster head, which is expressed as follows:

$$U_h = |\mathcal{A}| - \sum_{e\in A_h} \delta\left(e, A_j\right), \tag{9}$$

where $e \in A_h$ is a specific channel in spectrum band A_h, $|\mathcal{A}|$ is the cardinality of channel set $\mathcal{A}$. Moreover, the jamming indicator function $\delta\left(e, A_j\right)$ is expressed as follows:

$$\delta\left(e, A_j\right) = \begin{cases} 1, e \in A_j, A_j \subseteq \mathcal{A}_j, \\ 0, \text{otherwise}. \end{cases} \tag{10}$$

Equation 10 means that the utility of the cluster head h is the difference between the cardinality of channel set $\mathcal{A}$ and the jamming degree of current spectrum band strategy A_h. Hence, the optimization objective of the multi-leader sub-game is:

$$\mathbf{P}_2: \left(A_1^*, \cdots A_H^*\right) = \arg\max \sum_{h\in\mathcal{H}} U_h. \tag{11}$$

The above optimization objective means that each cluster head tries to find the optimal spectrum band that minimizes the cumulative jamming degrees. Then, we give the definition of NE, and we then prove that there exists at least one pure strategy NE in the multi-leader sub-game.

Definition 2 *The strategy combination* $\left(A_1^*, \cdots A_H^*\right)$ *is the pure strategy NE of the game if and only if no cluster head could enhance its utility via unilaterally changing its spectrum band selection strategy [34]:*

$$U_h\left(A_h^*, A_j\right) \geq U_h\left(A_h, A_j\right), \forall h \in H, \forall A_h \in \mathcal{A}_h \backslash A_h^*. \tag{12}$$

The above equation shows that for a specific jamming strategy A_j, the pure strategy NE improves the total network utility via unilaterally optimizing each cluster head's utility.

Theorem 1 *For a specific jamming strategy* A_j*, there exists at least one pure strategy NE* $\left(A_1^*, \cdots A_H^*\right)$ *with the following conditions:*

$$A_h^* = \mathcal{A}\backslash A_j, \forall h \in \mathcal{H}, A_j \in \mathcal{A}_j, \exists A_h^* \in \mathcal{A}_h. \tag{13}$$

Equation 13 depicts that the NE strategy of each cluster head changes with the variation of the jamming strategies.

Proof The proof by contradiction is applied for the multi-leader sub-game [29]. Assume that strategy combination $\left(A_1^*, \cdots A_H^*\right)$ is not the NE, which means $\exists h \in \mathcal{H}$ that satisfies $U_h\left(A_h^*, A_j\right) < U_h\left(A_h, A_j\right)$. Actually, unilaterally changing from A_h^* to A_h means that the cluster head h selects some channels that are jammed. Then, $\sum_{e\in A_h} \delta\left(e, A_j\right)$ increases, and

U_h decreases correspondingly. The above case depicts that the unilateral change does not satisfy $U_h\left(A_h^*, A_j\right) < U_h\left(A_h, A_j\right)$, and it is contradictory with the previous assumption. Thus, the proof of the above theorem has been completed. □

4.3 Multi-follower sub-game from the fine granularity

The objective of the multi-follower sub-game is to analyze and model the intra-cluster and inter-cluster competitive interactions among different cluster users. Note that the multi-leader sub-game is to guide the coarse-grained spectrum band selection of different cluster heads, and the multi-follower sub-game is to guide the fine-grained channel access of different users. Mathematically, the multi-follower sub-game is expressed as follows:

$$\mathcal{G}_{\mathrm{MF}} = \left\{\mathcal{H}, \{\mathcal{M}_h\}_{h\in\mathcal{H}}, \{\mathcal{A}_h\}_{h\in\mathcal{H}}, \left\{u_{h,k}\right\}_{h\in\mathcal{H},k\in\mathcal{M}_h}\right\}, \tag{14}$$

where $u_{h,k} = R_{h,k}$ denotes the throughput of the user k in the cluster h. In the multi-follower sub-game, only interference coordination needs to be considered after the multi-follower sub-game reaching NE for jamming strategy A_j.

Thus, the objective of the fine-grained multi-follower sub-game is:

$$\mathbf{P}_3: \left\{\left(a_{1,1}^*, \cdots a_{1,\mathcal{M}_1}^*\right) \ldots \left(a_{H,1}^*, \cdots a_{H,\mathcal{M}_H}^*\right)\right\} = \arg\max \sum_{h\in\mathcal{H}} \sum_{k\in\mathcal{M}_h} u_{h,k}. \tag{15}$$

The above optimization objective means that each user tries to find the optimal channel access strategy that maximizes the cumulative throughput of the clustering network.

Theorem 2 *For a specifical NE strategy* $\left(A_1^*, \cdots A_H^*\right)$ *when the jammer attacks band* A_j*, there exists at least one pure strategy NE* $\left\{\left(a_{1,1}^*, \cdots a_{1,\mathcal{M}_1}^*\right) \ldots \left(a_{H,1}^*, \cdots a_{H,\mathcal{M}_H}^*\right)\right\}$ *with the following condition:*

$$\begin{cases} \left\{\left(a_{1,1}^*, \cdots a_{1,\mathcal{M}_1}^*\right) \ldots \left(a_{H,1}^*, \cdots a_{H,\mathcal{M}_H}^*\right)\right\} = \underset{h\in\mathcal{H}}{\cup} A_h^* \cup \{0\}; \\ \mathcal{X} = \left\{x \middle| \forall x \in \mathcal{M}_h, m \in \{\mathcal{M}_h\}_{h\in\mathcal{H}} \backslash x, a_x^* \neq a_m^* \text{ if } \mathrm{P}_m \mathrm{d}_{m\to x}^{-\alpha} > \tau_{\mathrm{thres}}\right\}; \\ \forall x \in \mathcal{X}, a_x^* \notin A_j. \end{cases} \tag{16}$$

$a_{h,k} = 0$ means that the user keeps silent when strategy 0 is selected. The first line of Eq. 16 means that each user selects one channel from the optimal spectrum band of the cluster it belongs, or keeps silent. The second line depicts that neighboring users choose different channels to access when reaching NE. The third line illustrates that users avoid those jamming channels.

Proof Similarly, the proof by contradiction is also applied for the multi-follower sub-game. Assume that the strategy combination $\left\{\left(a_{1,1}^*, \cdots a_{1,\mathcal{M}_1}^*\right) \ldots \left(a_{H,1}^*, \cdots a_{H,\mathcal{M}_H}^*\right)\right\}$ is not one NE of the multi-follower sub-game, which means $\exists h \in \mathcal{H}, \exists k \in \mathcal{M}_k$ that satisfies $u_{h,k}\left(a_{h,k}^*, a_{-(h,k)}^*, A_j\right) < u_{h,k}\left(a_{h,k}, a_{-(h,k)}, A_j\right)$. Then, the throughput of the user k in cluster h can be rewritten as:

$$u_{h,k}\left(a_{h,k}^*, a_{-(h,k)}^*, A_j\right) = \begin{cases} B_{a_{h,k}^*} \log_2\left(1 + \frac{P_{h,k} d_{h,k}^{-\alpha}}{N_{a_{h,k}^*}}\right), \text{only user k in cluster } h \text{ selects } a_{h,k}^*, \\ 0, \text{otherwise.} \end{cases} \tag{17}$$

However, note that unilateral change from channel selection $a^*_{h,k}$ to $a_{h,k}$ causes the throughput of current user down to zero, as the conflict degree increases when breaking the equilibrium state. Thus, the above case means that $u_{h,k}\left(a^*_{h,k}, a^*_{-(h,k)}, A_j\right) < u_{h,k}\left(a_{h,k}, a_{-(h,k)}, A_j\right)$ can not be satisfied, and the above hypothesis is not valid. To sum up, the conclusion of Theorem 2 holds. □

Theorem 3 *For a specific jamming strategy A_j, there exists at least one SE in the proposed multi-leader multi-follower Stackelberg game.*

Proof In the above subsections, we proved that there exist at least one NE strategy combination $\left(A^*_1, \cdots A^*_H\right)$ for the leaders' sub-game, which maximizes the cumulative utility of all cluster heads, chooses optimal spectrum bands that are not jammed by the malicious jammer. In response to leaders' strategies, the follower sub-game shows that users can reach at least one NE strategy combination $\left\{\left(a^*_{1,1}, \cdots a^*_{1,\mathcal{M}_1}\right) \ldots \left(a^*_{H,1}, \cdots a^*_{H,\mathcal{M}_H}\right)\right\}$ which maximize the network throughput of cluster users. Combining Theorem 1, Theorem 2 and the definition of SE, we conclude that the proposed game has at least one SE. □

Figure 3 shows the operation process to obtain SE of the multi-leader multi-follower Stackelberg game. After observing the jamming strategy A_j, cluster heads (leaders) firstly adjust their spectrum band strategies to avoid the jamming attacks. Then, cluster users (followers) distributedly access channels after obtaining the spectrum band information sent by its cluster head. After that, cluster heads continue adjusting their band strategies until reaching the NE of the leader sub-game. When cluster users obtain the NE band strategy of their cluster heads, they adjust their channel access strategies until reaching

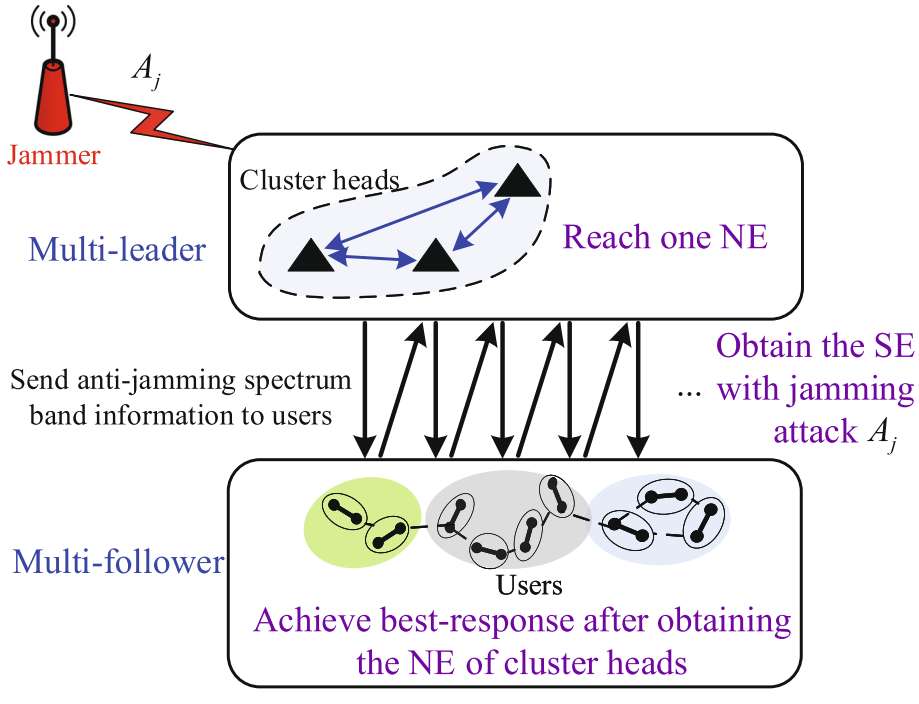

Fig. 3 The process of obtaining SE of the multi-leader multi-follower Stackelberg game

the best-response strategy (which is also the NE of the follower sub-game). In the process of continuous adjustment of cluster heads and cluster users, the system gradually reaches the SE for the current jamming strategy. A_j While with the dynamic changing of jamming attacks, different SEs can be achieved via the Stackelberg game iterations.

5 Hierarchical coordinated anti-jamming channel access algorithm

In this section, a hierarchical coordinated anti-jamming channel access (HCACA) algorithm is designed to obtain SEs of the multi-leader multi-follower Stackelberg game.

5.1 Slot structure

Before introducing the algorithm, we first design a slot structure for the operation of the hierarchical coordinated anti-jamming channel access, as shown in Fig. 4. At each time slot, actions are taken respectively for cluster heads and cluster users. Firstly, each cluster head observes the jamming signal, and maintains a corresponding strategy table for every jamming strategy. Secondly, each cluster head selects a spectrum band according to its strategy table. Then, all these cluster heads update their band strategies to avoid the current jamming signal. After the implementation of cluster heads, spectrum band strategies are sent to their cluster users, which means the first action for cluster users is the available channel acquisition. Each user will also maintain a specific strategy table for every jamming strategy to keep consistent with its cluster head, and it chooses one channel from its access table, which is randomly generated according to the information of the available channel. Once accessing the channel, each user transmission its data on the selected channel. When the transmission has been completed, users start updating their access strategies to avoid inter-cluster and intra-cluster conflicts among users.

5.2 Algorithm description

With the proposed slot structure, cluster heads and users update their spectrum band strategies and channel access strategies respectively using the hierarchical coordinated anti-jamming channel access (HCACA) algorithm. The detail of the HCACA algorithm description is shown in Algorithm 1.

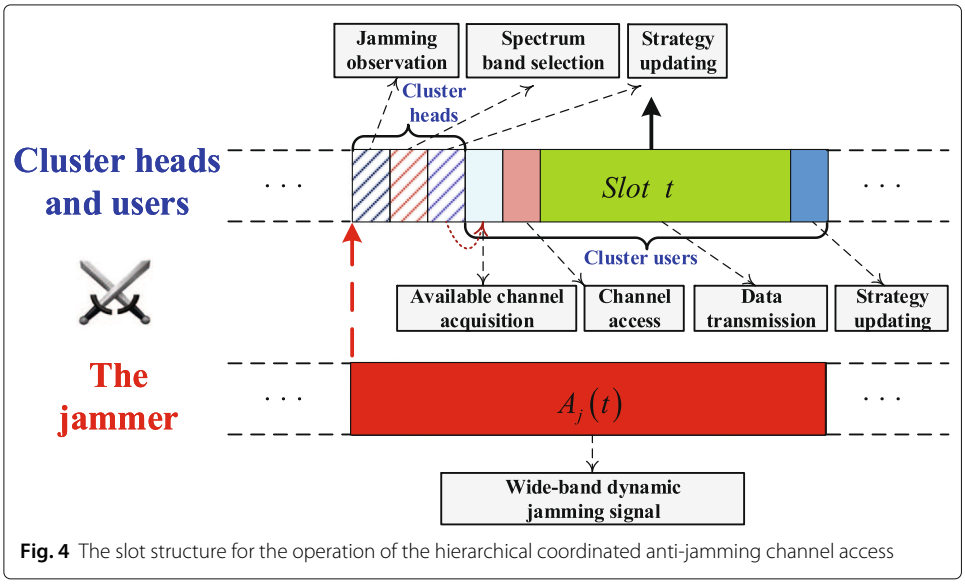

Fig. 4 The slot structure for the operation of the hierarchical coordinated anti-jamming channel access

Algorithm 1 : Hierarchical Coordinated Anti-jamming Channel Access Algorithm

Initialization: Set the maximal time slot T_{max}, the slot length, the channel set, the cluster set, the spectrum band strategy table $ATH_h = \left\{A_h\left(C_1\right), ..., A_h\left(C_{|\mathcal{A}_j|}\right)\right\}$ for cluster head $h, \forall h \in \mathcal{H}$, and the channel access table $AT_{h,k} = \left\{a_{h,k}\left(C_1\right), ..., A_{h,k}\left(C_{|\mathcal{A}_j|}\right)\right\}$ for user k in cluster $h, \forall h \in \mathcal{H}, k \in \mathcal{M}_h$.

Loop: $t = 1, ..., t, ..., T_{max}$

1. Jamming observation: Each cluster head observes current jamming signal A_j, and confirm corresponding coordination signal C_{A_j}.

2. Spectrum band selection: Each cluster selects one certain band strategy according to the recommended strategy $A_h\left(C_{A_j}\right)$.

3. Strategy updating of cluster heads: For each cluster h, it updates the band strategy according to the following rule:

$$A_h\left(C_{A_j}\right) = \begin{cases} 0, \ band\ A'\ is\ jammed\ (sensing); \\ A', \ band\ A'\ is\ available\ (sensing); \\ A_h\left(C_{A_j}\right), \ current\ selectedband\ is\ available; \\ 0, \ current\ selected\ band\ is\ jammed. \end{cases} \tag{18}$$

4. Available channel acquisition of users: Each user acquires the available channel set $A_h\left(C_{A_j}\right)$ from its cluster head h.

5. Channel access: Each user chooses one strategy $a_{h,k}\left(C_{A_j}\right)$ from its own strategy table, and $a_{h,k}\left(C_{A_j}\right) \in A_h\left(C_{A_j}\right) \cup \{0\}$.

6. Data transmission: Each user transmits on the selected channel, and judge wether the transmission is successful.

7. Strategy updating of users: For each user k in cluster h, it updates the channel access strategy according the following rule:

$$a_{n,k}\left(A_j\right) = \begin{cases} a', \ channel\ a'\ is\ idle\ (sensing); \\ 0, \ channel\ a'\ is\ busy\ (sensing); \\ a_{n,k}\left(A_j\right), \ successful\ transmission; \\ a_{n,k}\left(A_j\right), \ conflicting, \ with\ probability\ 1 - P_{back}; \\ 0, \ conflicting, \ with\ probability\ P_{back}. \end{cases} \tag{19}$$

8. If $t > T_{\max}$, the algorithm terminates.

End loop

The key steps of the proposed algorithm are the strategy updating processes of cluster heads and users, as shown in Eq. 18 and 19. In detail, when the cluster head h updates its strategy, it judges whether $A_h\left(C_{A_j}\right) = 0$. If $A_h\left(C_{A_j}\right) = 0$, then the cluster head chooses one spectrum band A' to sense [35]. If the sensing band is available (not jammed), then it sets $A_h\left(C_{A_j}\right) = A'$. Otherwise, it keeps $A_h\left(C_{A_j}\right) = 0$ if the sensed band is being jammed. Similarly, when user k in cluster h updates its strategy, it also judges whether $a_{n,k}\left(A_j\right) = 0$, and the sensing process of users are similar to cluster heads. However, if $a_{n,k}\left(A_j\right) \neq 0$, the current user will transmit on the selected channel, and keep strategy $a_{n,k}\left(A_j\right)$ unchanged for successful transmission. However, if conflicts occurs when transmitting, the user keeps its strategy with probability $1 - P_{\text{back}}$, or sets $a_{n,k}\left(A_j\right) = 0$ with probability P_{back}.

5.3 Complexity analysis

Motivated by [29], we analyze the complexity of the proposed HCACA algorithm, which is consisted of computational complexity and storage size.

First, we give the computation complexity under the fixed jamming. Note that each cluster head should observe the jamming signal A_j, and the corresponding complexity is $\mathcal{O}(Jo_1)$. Generally, (Jo_1) is a small constant which is related to the observation process. Hence, the computation complexity for jamming observation is $|\mathcal{H}|\,\mathcal{O}(Jo_1)$.

After the spectrum band selection, each cluster head needs to update their band strategy table ATH_h according to Eq. 18, and the computation complexity is $\mathcal{O}\left(B_{\mathrm{up1}}\right)$, where B_{up1} is a small constant related to the band updating process. Hence, the total computation complexity for band updating is $|\mathcal{H}|\,\mathcal{O}\left(B_{\mathrm{up1}}\right)$.

Following the updating process, each cluster head sends the band selection strategies to its cluster users, and then each user updates its channel strategy table according to Eq. 19, and the computation complexity is denoted as $\mathcal{O}\left(B_{\mathrm{up2}}\right)$. Thus, the total computation complexity for channel updating is $\mathcal{O}\left(\sum_{h\in\mathcal{H}}|\mathcal{M}_h|B_{\mathrm{up2}}\right)$. Assume that the convergence iterations is T_1 for the fixed jamming, and the total computation complexity is expressed as:

$$\mathrm{Comp}_{\mathrm{fixed}} = T_1\left[|\mathcal{H}|\,\mathcal{O}(Jo_1) + |\mathcal{H}|\,\mathcal{O}\left(B_{\mathrm{up1}}\right) + \mathcal{O}\left(\sum_{h\in\mathcal{H}}|\mathcal{M}_h|B_{\mathrm{up1}}\right)\right]. \tag{20}$$

Similarly, the computation complexity for the sweep jamming case is:

$$\mathrm{Comp}_{\mathrm{sweep}} = \left|\mathcal{A}_{\mathrm{sweep}}\right|T_1\left[|\mathcal{H}|\,\mathcal{O}(Jo_1) + |\mathcal{H}|\,\mathcal{O}\left(B_{\mathrm{up1}}\right) + \mathcal{O}\left(\sum_{h\in\mathcal{H}}|\mathcal{M}_h|B_{\mathrm{up1}}\right)\right], \tag{21}$$

where $\mathcal{A}_{\mathrm{sweep}}$ is the strategy set of the sweep jammer.

While the computation complexity for the random jamming case is:

$$\mathrm{Comp}_{\mathrm{random}} = |\mathcal{A}_{\mathrm{random}}|^2 T_1\left[|\mathcal{H}|\,\mathcal{O}(Jo_1) + |\mathcal{H}|\,\mathcal{O}\left(B_{\mathrm{up1}}\right) + \mathcal{O}\left(\sum_{h\in\mathcal{H}}|\mathcal{M}_h|B_{\mathrm{up1}}\right)\right], \tag{22}$$

where $\mathcal{A}_{\mathrm{random}}$ is the strategy set of the sweep jammer. Note that the random jammer randomly selects one strategy from its jamming strategy at each time, thus average $O\left(|A_{\mathrm{random}}|^2 T_1\right)$ iterations will be necessary for the convergence of the proposed HCACA algorithm (According to [28] Lemma 3).

Moreover, cluster heads and cluster users should store their band strategy tables and channel strategy tables respectively. Thus, the storage size is:

$$\mathrm{Store}_j = \left|\mathcal{A}_j\right|\left[|\mathcal{H}|\,O(St_1) + \mathcal{O}\left(\sum_{h\in\mathcal{H}}|\mathcal{M}_h|St_2\right)\right], \tag{23}$$

where $\mathcal{A}_j$ denotes different jamming strategy sets for different jamming patterns (1, $\mathcal{A}_{\mathrm{sweep}}$ or $\mathcal{A}_{\mathrm{random}}$) , St_1 is a small constant which is related to the size of band strategy

table for one jamming strategy, and St_2 is a small constant with respect to the size of channel strategy table for one jamming strategy.

It is summarized that the computational complexity at each slot is a small constant, and the storage size is not too large as is mentioned above. In a word, the proposed HCACA algorithm has low complexity, and the approach can be implemented using typical technologies.

6 Simulation results and discussions

In this section, the simulations are conducted, and then some discussions with respect to simulation results are made.

6.1 Setting of parameters

First, the details of parameters are given, as shown in Table 1. Here, users randomly locate in an area of 12 km $\times$ 12 km, and different users may belong to different clusters. A typical scenario of the clustering network is shown in Fig. 5, where there exist 4 clusters and 24 users. In each cluster, there is a cluster head and 6 users (transmitter-receiver pairs). Users are influenced by the intra-cluster interference and inter-cluster interference if they choose the same channel to transmit data. It is assumed that the bandwidth of each channel is 2 MHz, the transmission power of each user is 0.1 W, the path-loss factor is assumed to be 3, and the background noise power is $-$ 100 dBm. Besides, the interference distance is set to be 2000 m, which is positively related to the interference threshold τ_{thres}. Besides, the time is slotted, and the duration of one time slot is 10 ms. In detail, the duration of jamming observation, spectrum band selection, strategy updating of the cluster head, available channel acquisition, channel access and strategy updating of users are set to be 0.5 ms, and the duration of data transmission is 7 ms. Furthermore, the clustering network is under the attack of a malicious jammer, and three different wide-band jamming patterns are considered, i.e., the fixed jamming, the sweep jamming and the random jamming, as shown in Fig. 6.

6.2 Convergence analysis

Secondly, the convergence performance of the proposed HCACA algorithm is depicted in this subsection. Here, simulations are conducted under these three jamming patterns mentioned above. In detail, Fig. 7 shows the convergence process of the network throughput with fixed, sweep and random wide-band jamming (At each time slot, the jammer chooses 5 continuous channels to attack). It can be concluded that the proposed HCACA algorithm converges with the fastest speed under fixed jamming, as it is much easier for

Table 1 Parameters settings in simulations

T_{slot}	10 ms
$T_{\text{jo}}, T_{\text{bs}}, T_{\text{suh}}, T_{\text{acc}}, T_{\text{ca}}, T_{\text{suu}}$	0.5 ms
T_{tr}	7 ms
$\boldsymbol{\mathcal{A}}$	12
Number of users	24
$\boldsymbol{\mathcal{B}}_{a_{h,k}}$	2 MHz
$P_{h,k}$	0.1 W
α	3
$N_{a_{h,k}}$	-100 dBm.
P_{back}	0.5

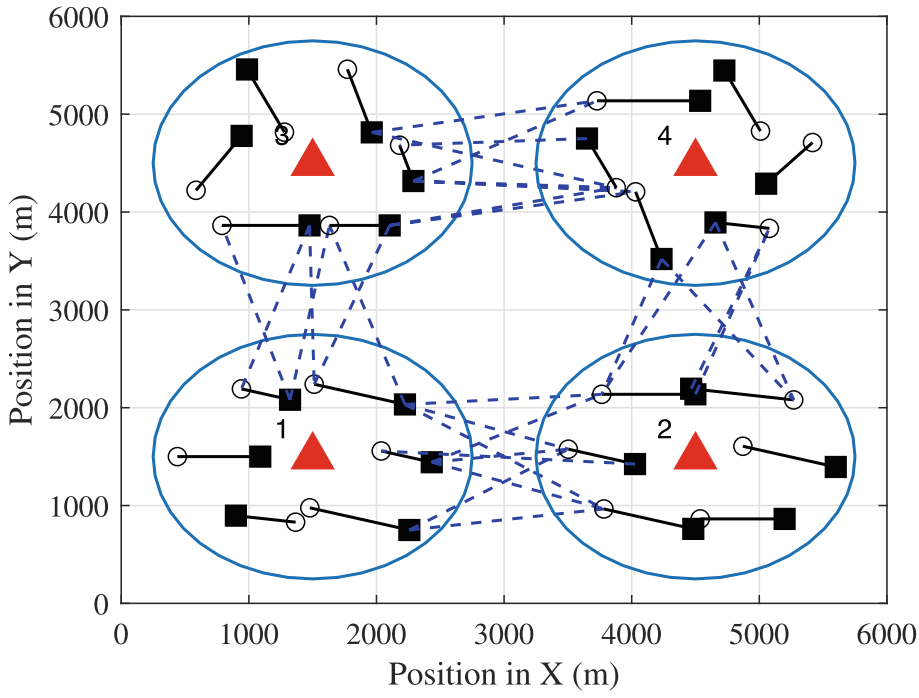

Fig. 5 The network topology of the clustering network (4 clusters with 24 users)

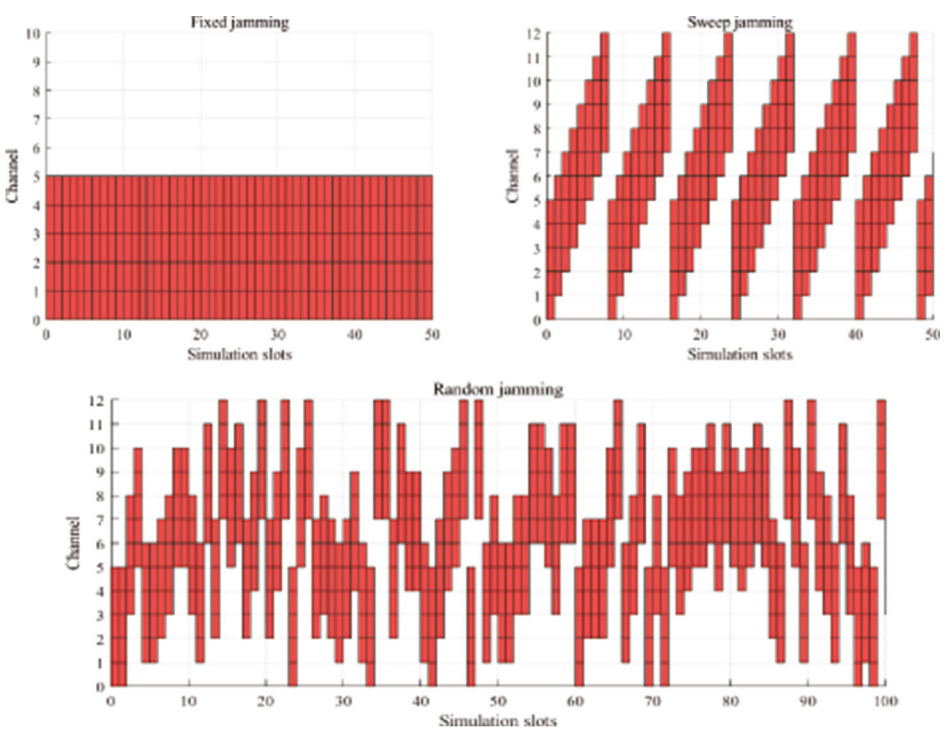

Fig. 6 Different jamming patterns with wide-band spectrum characteristics

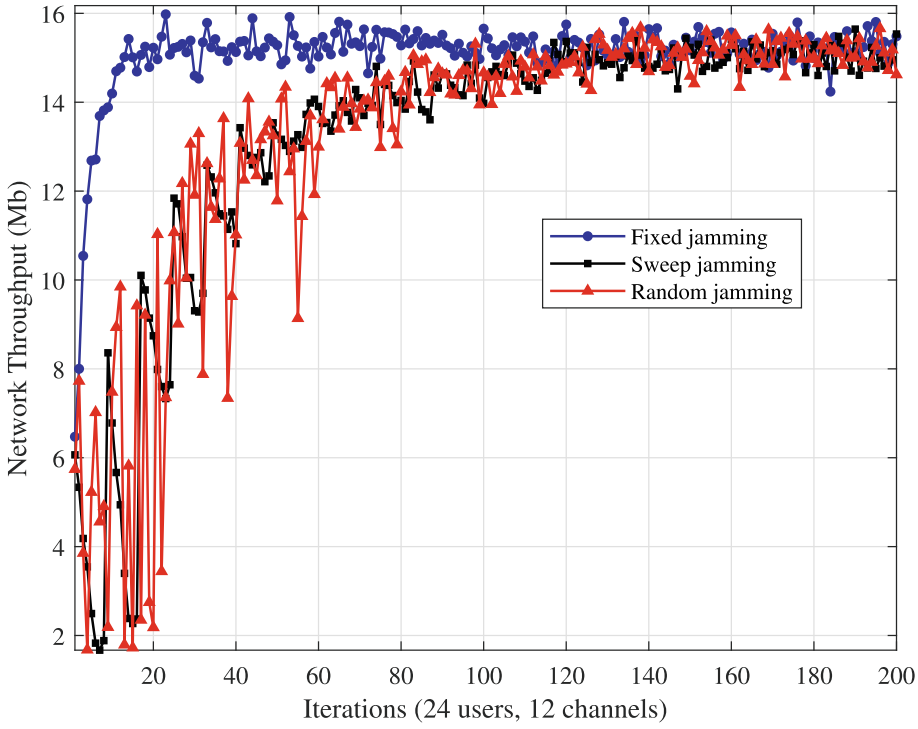

Fig. 7 The network throughput under different jamming patterns

cluster heads to avoid the fixed jamming, and for users to coordinate the internal conflicts. Besides, the convergence time increases with the increase of the dynamic characteristic of the jammer as we can see that the proposed algorithm converges slower under the random jamming than under the sweep jamming. Note that in the initial stage, the network throughput fluctuates acutely under the sweep jamming and the random jamming, as the jamming state varies as time goes by. While with the updating of the strategy tables, the network throughput converges gradually. In a word, it depicts that the proposed algorithm is well-adapted to the dynamic and wide-band jamming environment. Moreover, the existence of channel fading also leads to slight fluctuations in network throughput; however, this phenomenon does not affect the convergence process of the HCACA algorithm.

6.3 Performance comparison

To further investigate the performance of the proposed approach, four different algorithms are compared in this subsection, the hierarchical coordinated anti-jamming algorithm HCACA, the distributed anti-jamming learning algorithm (DAL), the coordinated learning algorithm proposed in [36], and the random selection algorithm [37]. Here, users in the DAL algorithm first utilize the jamming signal as the coordination signal, and distributedly update their channel access strategies according to Eq. 19. While users in the coordinated learning algorithm adopt random integers as coordination signals, and avoid collision via distributed learning. Moreover, users in the random selection algorithm randomly select a channel from their channel set to access.

Figures 8 and 9 show the performance comparison under the sweep wide-band jamming and the random wide-band jamming. As shown in Fig. 8, it is concluded that the proposed

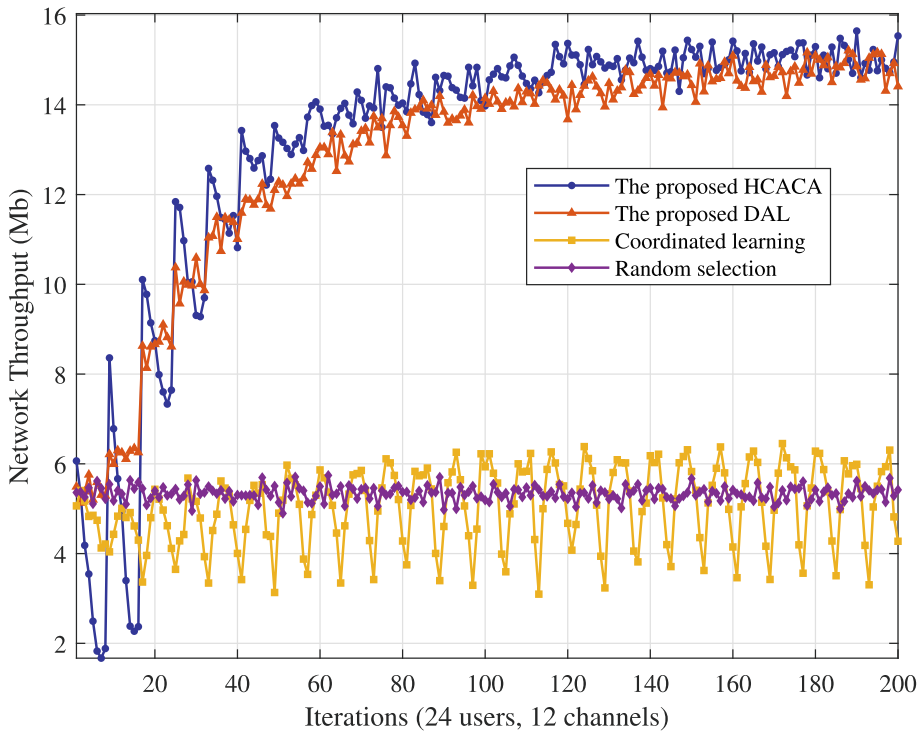

Fig. 8 The performance comparison among four different algorithms under sweep jamming

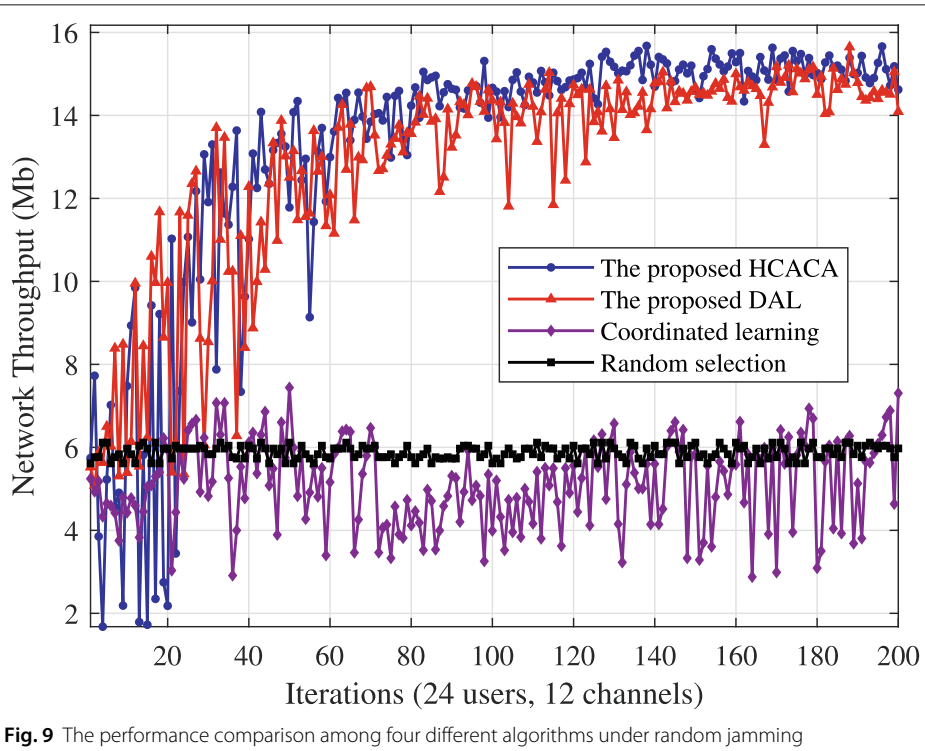

Fig. 9 The performance comparison among four different algorithms under random jamming

HCACA outperforms other comparative algorithms and achieves the highest throughput with the fastest convergence speed under the sweep wide-band jamming. Note that the proposed DAL algorithm also performs well compared with the coordinated learning algorithm and the random selection algorithm, which shows the advantage of jamming signal utilization. Besides, due to that the coordinated algorithm adopts random integers as coordination signals, it can not adapt to the dynamic wide-band jamming well. Thus, the throughput with coordination learning fluctuates and does not converge to a stable state. Similarly, Fig. 9 depicts that the proposed HCACA algorithm has good adaptive capacity under random jamming. In detail, the proposed HCACA algorithm adapts to the stochastic behavior of the random jamming and converges gradually. The proposed DAL algorithm also performs well thanks to the observation of jamming signals. While the coordination learning algorithm and the random selection algorithm are hard to accommodate the random jamming and obtain relatively low network throughput than proposed algorithms.

To analyze the advantage in convergence speed of the proposed HCACA algorithm and DAL algorithm. Here we count the convergence time of 100 times Monte Carlo experiments, and then take the average value when reaching the equilibrium strategy combination of the network (for the HCACA algorithm, different SEs are achieved, while for the DAL algorithm, NEs are achieved for different jamming attacks). As shown in Fig. 10, the proposed hierarchical coordinated anti-jamming approach with Stackelberg game formulation converges more faster than the distributed anti-jamming learning approach under three different wide-band jamming attacks. The reason is that the proposed HCACA approach avoids jamming attacks via the cluster heads, and it reduces the strategy space greatly. In addition, it is also illustrated that with the increase of the dynamic and random characteristic of the jamming attacks, the average iterations increases accordingly, however, the proposed hierarchical anti-jamming approach still outperforms the distributed anti-jamming approach in terms of convergence speed.

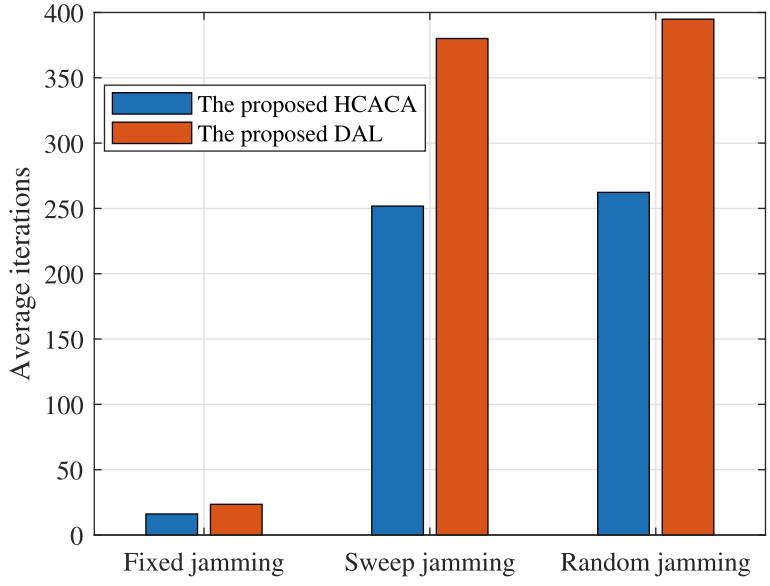

Fig. 10 The comparison of average convergence time between two different algorithms

Table 2 Summary of main notations

$\mathcal{H}$	Set of clusters
$\mathcal{M}_h$	Set of users in cluster h
$\mathcal{A}$	Set of channels
$a_{h,k}$	Channel selection action of user k in cluster h
$\mathcal{B}_{a_{h,k}}$	Channel bandwidth
$P_{h,k}$	Transmission power of user k in cluster h
$d_{h,k}$	Transmission distance
α	Path loss factor
$N_{a_{h,k}}$	Noise power of channel $a_{h,k}$.
$\delta\left(a_n\left(t\right)\right)$	Jamming-interference conflict indicator function
$\Delta\left(a_{h,k}, a_{-(h,k)}, A_j\right)$	Cumulative jamming-interference indicator function
$a_{-(h,k)}$	Channel access strategy combination of all users except the kth user in cluster h
A_j	Jamming strategy
$R_{h,k}$	Throughput of user k in cluster h
U_h	Utility function of cluster head h
$u_{h,k}$	Utility function of user k in cluster h
C_{A_j}	Coordination signal when jammer attacks A_j
P_{back}	Probability of backoff t
$T_{\max}$	Maximal iterations of the algorithm

7 Conclusion

This paper investigated the multi-user coordinated anti-jamming problem in clustering communication networks. A hierarchical coordinated anti-jamming approach was proposed, and a multi-leader multi-follower Stackelberg game was introduced to model the anti-jamming problem. In detail, cluster heads acted as leaders, and selected available frequency bands to avoid jamming attacks. While users in each cluster acted as followers, and selected corresponding channels distributedly and independently. Moreover, it was proved that there exist multiple Stackelberg equilibriums (SEs) in the proposed game. To obtain SEs, a hierarchical coordinated anti-jamming channel access (HCACA) algorithm was designed. Simulation results illustrated that the proposed approach is effective to cope with the dynamic wide-band jamming attacks. Furthermore, it was also depicted that the proposed approach outperforms the distributed anti-jamming comparative approach in terms of convergence speed.

Abbreviations
A summary of main notations is given in Table 2.

Acknowledgements
The authors would like to thank Dr. Ximing Wang for discussions on the system model.

Authors' contributions
Yifan Xu, Jin Chen conceived the system model. Yifan Xu, Zhibin Feng and Kailing Yao completed the game-theoretic analysis of this paper. Yifan Xu, Guoxin Li, Fei Song and Gui Fang contributed to the algorithm design. Yifan Xu also performed the simulations with Zhibin Feng. Besides, Yifan Xu, Jin Chen and Zhibin Feng wrote the manuscript. The authors read and approved the final manuscript.

Authors' information
Not applicable.

Funding
This work was supported by the National Natural Science Foundation of China under 62071488 and 61771488.

Availability of data and materials
Not applicable.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: 7 May 2021 Accepted: 5 July 2021
Published online: 19 July 2021

References

1. X. Lu, L. Xiao, C. Dai, H. Dai, UAV-aided cellular communications with deep reinforcement learning against jamming. IEEE Wirel. Commun. **27**, 48–53 (2020)
2. L. Xiao, X. Lu, T. Xu, et al., Reinforcement learning based mobile offloading for edge computing against jamming and interference. IEEE Trans. Commun. **68**, 6114–6126 (2020)
3. X. Wang, J. Wang, et al., Dynamic spectrum anti-jamming communications: Challenges and opportunities. IEEE Commun. Mag. **58**, 79–85 (2020)
4. Q. Wu, T. Ruan, et al., A unified cognitive learning framework for adapting to dynamic environment and tasks. arXiv preprint arXiv:2106.00501 (2021). https://arxiv.org/abs/2106.00501
5. Z. Han, D. Niyato, W. Saad, T. Başar, A. Hjørungnes, Game theory in wireless and communication networks: theory, models, and applications (Cambridge university press, 2012)
6. Y. Xu, A. Anpalagan, Q. Wu, et al., Decision-theoretic distributed channel selection for opportunistic spectrum access: Strategies, challenges and solutions. IEEE Commun. Surv. Tutor. **15**, 1689–1713 (2013)
7. D. T. Hoang, X. Lu, D. Niyato, P. Wang, D. I. Kim, Z. Han, Applications of repeated games in wireless networks: A survey. IEEE Commun. Surv. Tutor. **17**, 2102–2135 (2015)
8. J. Zheng, H. Zhang, Y. Cai, et al., Game-theoretic multi-channel multi-access in energy harvesting wireless sensor networks. IEEE Sensors J. **16**, 4587–4594 (2016)
9. Y. Xu, J. Wang, Q. Wu, J. Zheng, et al., Dynamic spectrum access in time-varying environment: Distributed learning beyond expectation optimization. IEEE Trans. Commun. **65**, 5305–5318 (2017)
10. C. Yang, J. Li, P. Semasinghe, E. Hossain, S. M. Perlaza, Distributed interference and energy-aware power control for ultra-dense D2D networks: A mean field game. IEEE Trans. Wirel. Commun. **16**, 1205–1217 (2017)
11. Y. Zhang, C. Jiang, J. Wang, Z. Han, et al., Coalition formation game based access point selection for lte-u and wi-fi coexistence. IEEE Trans. Ind. Informat. **14**, 2653–2665 (2018)
12. Y. Hu, A. Sanjab, W. Saad, Dynamic psychological game theory for secure Internet of battlefield things (IoBT) systems. IEEE Internet Things J. **6**, 3712–3726 (2019)
13. J. Moura, D. Hutchison, Game theory for multi-access edge computing: survey, use cases, and future trends. IEEE Commun. Surv. Tutor. **21**, 260–288 (2019)
14. J. Cao, T. Peng, Z. Qi, et al., Interference management in ultradense networks: A user-centric coalition formation game approach. IEEE Trans. Veh. Technol. **67**, 5188–5202 (2018)
15. D. Yang, J. Zhang, X. Fang, et al., Optimal transmission power control in the presence of a smart jammer. IEEE GLOBECOM, 5506–5511 (2012)
16. D. Yang, G. Xue, J. Zhang, et al., Coping with a smart jammer in wireless networks: A Stackelberg game approach. IEEE Trans. Wirel. Commun. **12**, 4038–4047 (2013)
17. L. Xiao, T. Chen, J. Liu, H. Dai, Anti-jamming transmission Stackelberg game with observation errors. IEEE Commun. Lett. **19**, 949–952 (2015)
18. L. Jia, F. Yao, Y. Sun, et al., Bayesian Stackelberg game for anti-jamming transmission with incomplete information. IEEE Commun. Lett. **20**, 1991–1994 (2016)
19. L. Jia, F. Yao, Y. Sun, et al., A hierarchical learning solution for anti-jamming Stackelberg game with discrete power strategies. IEEE Wirel. Commun. Lett. **6**, 818–821 (2017)
20. Y. Xu, G. Ren, J.in. Chen, et al., A one-leader multi-follower Bayesian-Stackelberg game for anti-jamming transmission in UAV communication networks. IEEE Access. **6**, 21697–21709 (2018)
21. N. Qi, W. Wang, M. Xiao, et al., A learning-based spectrum access Stackelberg game: Friendly jammer-assisted communication confrontation. IEEE Trans. Veh. Technol. **70**, 700–713 (2021)
22. Y. Li, L. Xiao, J. Liu, et al., Power control Stackelberg game in cooperative anti-jamming communications. GAMENETS, 1–6 (2014)
23. Y. Yuan, T. Yang, H. Feng, et al., An iterative matching-Stackelberg game model for channel-power allocation in D2D underlaid cellular networks. IEEE Trans. Wirel. Commun. **17**, 7456–7471 (2018)
24. D. N. Duong, S. A. Madhukumar, D. Niyato, Stackelberg bayesian game for power allocation in two-tier networks. IEEE Trans. Veh. Technol., 2341–2354 (2016)
25. Z. Su, N. Qi, Z. Du, et al., Guarding legal communication with smart jammer: Stackelberg game based power control analysis. China Commun. **18**, 126–136 (2021)
26. K. I. Ahmed, O. A. Fapojuwo, Stackelberg equilibria of an anti-jamming game in cooperative cognitive radio networks. IEEE Trans. Cogn. Commun. Netw. **4**, 121–134 (2018)
27. C. Han, L. Huo, X. Tong, et al., Spatial anti-jamming scheme for internet of satellites based on the deep reinforcement learning and Stackelberg game. IEEE Trans. Veh. Technol. **69**, 5331–5342 (2020)
28. L. Cigler, B. Faltings, in *10th International Conference on Autonomous Agents and Multiagent Systems*, Reaching correlated equilibria through multiagent learning, vol. 2, (Taipei, 2011), pp. 509–516

29. Y. Xu, Y. Xu, X. Dong, et al., Convert harm into benefit: A coordination-learning based dynamic spectrum anti-jamming approach. IEEE Trans. Veh. Technol. **69**, 8–13032 (2020)
30. P. Neamatollahi, S. Abrishami, M. Naghibzadeh, et al., Hierarchical clustering-task scheduling policy in cluster-based wireless sensor networks. IEEE Trans. Ind. Informat. **14**, 1876–1886 (2018)
31. C. Singhal, S. De, in *Advances in Wireless Technologies and Telecommunication (AWTT)*, Resource allocation in next-generation broadband wireless access networks (IGI Global, Hershey, 2017)
32. Y. Xu, J. Wang, Q. Wu, A. Anpalagan, et al., Opportunistic spectrum access in unknown dynamic environment: A game-theoretic stochastic learning solution. IEEE Trans. Wirel. Commun. **11**, 1380–1391 (2012)
33. Y. Sun, J. Wang, F. Sun, et al., Energy-Aware joint user scheduling and power control for two-tier femtocell networks: A hierarchical game approach. IEEE Syst. J. **12**, 2533–2544 (2018)
34. K. Yao, J. Wang, Y. Xu, et al., Self-organizing slot access for neighboring cooperation in UAV swarms. IEEE Trans. Wirel. Commun. **19**, 2800–2812 (2020)
35. J. Wang, G. Ding, Q. Wu, et al., Spatial-temporal spectrum hole discovery: A hybrid spectrum sensing and geolocation database framework. Chinese Sci. Bull. **59**, 1896–1902 (2014)
36. L. Wang, K. Wu, M. Hamdi, et al., Attachment-learning for multi-channel allocation in distributed ofdma-based networks. IEEE Trans. Wirel. Commun. **12**, 1712–1721 (2013)
37. D. Shen, O. V. Li, Stabilized multi-channel aloha for wireless OFDM networks. IEEE GLOBECOM. **1**, 701–705 (2002)

Publisher's Note