Wang *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:211
DOI 10.1186/s13638-016-0702-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Distributed coalitional game for friendly jammer selection in ultra-dense networks

Ying Wang[1*], Zhongyu Miao[1], Ruijin Sun[1] and Lei Jiao[2]

Abstract

Consider an ultra-dense heterogeneous network with one malicious eavesdropper intercepting macro-layer information. A portion of small-cell base stations (SBSs) acts as the friendly jammer to help improving macro-users' secrecy rate by transmitting interference signal on the wiretap channel. In return, the client macro-user pays to its jammers for the jamming power that they provide. Instead of transmitting noise as traditional jammers do, this paper proposes a modified spectrum leasing method, which allows SBSs to replace the thermal noise with their own traffic. This approach also permits the jamming SBSs to access extra spectrum in order to enhance the performance. In the considered scenario, the macro-user tries to find the SBSs that can mostly protect its confidential message, while each SBS decides whether to serve as a jammer or not. Once an SBS decides to be a jammer, it needs to choose the optimal client macro-user depending on the channel condition. This two-way selection problem between SBSs and macro-users is modeled as the coalition formation game with non-transferable utility, and a distributed scheme is proposed for this game, in which the players (macro-users and SBSs) individually make a decision and converge to a Nash-stable partition in a self-organized manner. The simulation results show that the majority of macro-user equipments enjoy a fivefold increment in average secrecy rate and that the friendly jammer scheme effectively protects the macro-users from the eavesdropper. At the same time, the average capacity of small-cell layer also achieves a 16.92 % improvement.

Keywords: Ultra-dense networks, Friendly jammer, Information security, Coalition formation game

1 Introduction

With the proliferation of the smart and real-time devices, the demands for mobile data rise dramatically, which has promoted a large amount of hotspots in indoor areas. It is estimated that global wireless traffic will continue growing and reach a level that is 1000 times larger than nowadays in a decade [1]. The communication system is facing an unprecedented challenge. As a result, the technology of ultra-dense networks (UDNs) is introduced as a promising approach to satisfy the skyrocketed user demands and to improve indoor coverage and spectrum efficiency. A UDN is composed of a macrocell overlayed by a number of densely deployed low-power, low-cost base stations which could provide high throughput for indoor and hotspot areas. The two-tier architecture has the advantage of ensuring the overall coverage as well as satisfying the local traffic demand. UDN is viewed as one of the key technologies in 5G, and fruitful achievements have been made in fields of interference management [2–4], power control [5–7], energy efficiency [8–10], offloading [11, 12], network selection [13, 14], etc.

Meanwhile, information security is an important aspect in communications. However, there are few articles related to security and privacy in UDNs. Traditionally, the way to improve confidentiality of the information mainly relies on the encryption system at higher layers. However, the computational cost for either encryption or the decryption is usually so high that it may be a great burden for both the SBSs and macrocell user equipments (MUEs), especially for the small-cell infrastructures [15]. As the wireless and mobile network structure becomes more and more complicated, the key management is far more difficult as the number of nodes increases [16]. What is more, the broadcast nature of the wireless channel makes it unsafe for key distribution which is fatal to most of the encryption algorithms since the opponent can easily deci-

*Correspondence: wangying@bupt.edu.cn
[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China
Full list of author information is available at the end of the article

pher the transferred message once the key is overheard. Hence, it is discovered in recent years that it may not be so efficient or suitable to rely on the upper layer encryption in wireless networks. A wiretap channel is introduced in [17], and it is proven that if the wiretap channel was worse than the main channel, the users could have a nonzero secrecy capacity. This pioneer work have enlightened the research on physical layer security, which has recently been discovered as an efficient way to fight against the malicious eavesdroppers. One of the basic methods of improving the legitimate users' secrecy capacity in physical layer security is interfering the eavesdropper through the artificial noise, which is called friendly jamming or cooperative jamming. More specifically, in the regime of friendly jamming, there are numbers of friendly jammers in the network responsible for transmiting noise or the codewords on the same channel of the client user's so as to confuse the eavesdropper and, thus, enhance the safety performance of the legitimate user.

Most of the current studies on friendly jammer are carried out within relay [18–21] and cognitive scenarios [22–24]. Article [19] studies a two-way relay system with an untrusted relay node. The transmission pair improves its secrecy rate by buying proper jamming power from the friendly jammers. In [20], a coalition formation game is formulated to investigate the cooperation between relays and friendly jammers in order to assist data transmission. The drawback of those schemes is the requirement for installation and maintenance of the dedicated jammers, resulting in a significant cost to the operator. A friendly jamming paradigm using spectrum leasing is developed in [22], where the jammers are unsubscribed nodes that also have data to transmit. The subscribed user attracts the jammers' cooperation by allowing them to use a fraction of its frame for their own data transmissions. In [23], a new cooperative scheme is introduced in a cognitive network with several relay nodes. The secondary users (SUs) are allowed to transmit simultaneously with the primary user (PU). In the first hop, the SU transmitter sends its information to the relay while the SU receiver acts as a friendly jammer. In the second hop, the relay passes the information to the SU receiver and the transmitter, in turn, takes the role of disturbing the eavesdropper. Nonetheless, most existing work on friendly jammer is based on a relatively simple network topology, which considers only one transmission pair (i.e., a source and a destination). Studies in [25–27] investigate the power allocation of the friendly jammer in a network with multiple source-destination links, but there is only one jammer in the system. All those abovementioned approaches and scenarios are not suitable for UDNs. In UDNs, several macro base station (MBS)-MUE links need to keep their messages secret. Furthermore, the densely distributed SBSs can be employed as friendly jammers to help MUEs with secure communication, which avoids deploying dedicated jammers. Hence, friendly jammer via SBSs is an appropriate method to enhance the security of UDNs.

As mentioned previously, existing approaches do not apply directly to UDNs due to the fact that both the users and jammers have more than one candidate servers or clients. When there is only one source-destination link, the jammers do not need to consider which pair to choose, nor do the transmission pair in the situation where exists only one jammer. Nevertheless, in UDNs, the MUEs compete for the most effective jammers from multiple SBSs for themselves, while the SBSs carefully estimate the revenue from different MUEs and choose the one that brings the maximum benefits as a client user. This generates a two-way selection problem, making it more difficult to form the cooperative structure between the users and jammers. Therefore, extensions and modifications are needed to model the two-way selection among the multiple MUEs and jammers. Furthermore, jammers in previous studies have no resource to transmit data. They obtain the transmission opportunity as the resource reward for providing jamming service to the transmission pair, as in [22, 23]. More specifically, the jammers in the previous studies do not have any chance to serve their own traffic unless if they provide jamming service. Hence, the jammers in existing articles have strong motivation to perform cooperative jamming, which is not the case in UDNs. The SBSs have their own users and limited resource. Providing friendly jamming means a loss of performance for SBSs since they allocate part of their power to jamming and concentrate less on their own users. Consequently, the SBSs need to weigh the income against the performance loss and may not be so willing to help. A more powerful mechanism of reimbursement is required to encourage the SBSs to cooperate as well as to enhance their performance when they provide the jamming service. In addition, interference has always been a problem in UDNs. Though friendly jammer takes advantage of interference to protect privacy, a careful balance among all kinds of interferences is also required to guarantee the overall performance of the network. Therefore, the introduction of friendly jammer to UDNs is a more intricate problem. To our best knowledge, it is the first work to apply friendly jammer to UDNs.

The enormous number of nodes in UDNs makes it complicated for a centralized algorithm to handle such a large amount of data and computations. Game theory is a powerful tool for analyzing the interaction between various players. Each player in the game can, based on network condition, make a decision without the instruction of a centralized control node. Modeling interactions among users as a game and designing distributed algorithms accordingly have been widely applied in communication systems [5, 8, 11–13]. Coalition formation game is one

of the most important classes in game theory, which can be used to form win-win or cooperative coalitions among the players to optimize the network performance and to improve their own benefits at the same time [20, 28, 29].

This paper tries to provide an insight about the future practical use of friendly jamming techniques and investigates the secure communication in UDNs with an eavesdropper, making use of the SBSs in the network to prevent the eavesdroppers from overhearing the information between MBS and MUEs. The MUEs compete for the jammers which can provide the maximum increase in secrecy capacity. On the other hand, the SBSs also have the freedom to decide whether to be a jammer or not and to choose its client user in order to optimize its own utilization. The interaction between MUEs and SBSs has been modeled as a coalition formation game. According to the role that SBSs and MUEs play in this friendly jammer system, we use SBS and jammer interchangeably in the following pages, as well as MUE and user (or client user).

The main contributions of this paper are as follows:

- This paper extends the application of friendly jammer to a more realistic network scenario with multiple users (i.e., MUEs) and multiple jammers (i.e., SBSs). Furthermore, a novel-distributed scheme is proposed to solve the two-way selection problem among users and jammers, by exploiting the non-transferable utility (NTU) coalition formation game.
- Since it is reasonable for SBSs to attach more importance to performance than to the money paid by MUEs, in addition to compensating the SBSs for the jamming power, a modified stage combined spectrum leasing (SCSL) is proposed to effectively motivate the SBSs to cooperate. Besides, SCSL allows jammers to replace noise with useful information as the interference signal to eavesdropper, which makes best use of the resource and greatly improves the efficiency.

The rest of this paper is organized as follows. In Section 2, the system model is presented. Section 3 formulates the problem in a coalitional game approach and solves it in a distributed manner. The property of stabilization is also proven in this section. Numerical results are displayed and discussed in Section 4 before we conclude the paper in Section 5.

2 System model

In this section, we first describe the network model of the proposed scheme. Then, the mechanism of the friendly jammer is introduced and a brief analysis of the mechanism is presented. At last, we explain the SCSL and discuss how it can improve the performance compare with the spectrum leasing [22, 30].

2.1 Network model

Consider an ultra-dense network with an eavesdropper, an MBS, densely deployed small cells, and several MUEs. We assume that the index of the MBS is 0 sand that of the eavesdropper is e. Let $\mathbb{M} = \{1, 2, \ldots, M\}$ and $\mathbb{K} = \{1, 2, \ldots, K\}$ be the set of M MUEs and K SBSs in the network, respectively, where $M = |\mathbb{M}|$ and $K = |\mathbb{K}|$. Each SBS k serves only one small-cell user equipment (SUE), denoted by v_k. The spectrum access strategies between the two layers can be divided into three classes: (1) shared, i.e., the small cells are allowed to reuse the entire bandwidth of MBS, which has a high level of resource utilization but relatively severe cross and co-layer interference; (2) dedicated, i.e., a dedicated spectrum that are orthogonal to that of macrocell's is allocated to the small cells, which eliminates the cross-layer interference at the cost of a lower level of resource utilization; (3) hybrid, i.e., a portion of the macrocell's spectrum is allocated to a small cell, which is a compromise of interference and resource reuse. To eliminate the cross-layer interference, we assume a dedicated mode as the basic spectrum access strategy between the two layers. Assuming that there are N orthogonal subchannels of bandwidth W and let $\mathbb{N} = \{1, 2, \ldots, N\}$ represent all the frequency resource available in the system. In a dedicated spectrum allocation, the $\mathbb{N}$ is divided into two disjoint sets N_m and N_k, where $N_m \cap N_k = \emptyset$ and $N_m \cup N_k = \mathbb{N}$. The MBS chooses one subchannel n_m from N_m to serve MUE m, $m \in \mathbb{M}$ and SBS k, $k \in \mathbb{K}$ transmits on $n_k \in N_k$ to serve its user. Since there are far more SBSs than the subchannels that dedicated to SBSs, it is indispensable to reuse the subchannels in N_k and thus the co-layer interference among co-channel SBSs is generated. Denote by $I(n)$ the set of SBSs that use the same channel $n \in N_k$, $I(n) = \{n_k = n, k \in \mathbb{K}\}$. The channel model includes the path loss and Rayleigh fading [20]. Let $h^n_{i,j}$ be the channel gain between the transmitter i and the receiver j on subchannel n. We assume that the channel gains in the system can be measured (including those of channels to the eavesdropper) [22]. The values of maximum power of MBS and SBS are P_0 and P_{sbs}, respectively. The transmission power of SBS k on subchannel n is denoted by P^n_k. The power of thermal noise is σ^2.

The macrocell users require their information being safely transmitted, and they try to maximize their secrecy capacity while the SUEs do not require that. Secrecy capacity is defined as the achievable capacity of the receiver excluding the capacity overheard by the eavesdropper. Suppose the base stations transmit at full power, the capacity of MUE m on subchannel n_m is given by

$$\gamma_m^{n_m} = \frac{W}{2}\log_2\left(1 + \frac{P_0 h_{0,m}^{n_m}}{\sigma^2}\right), \tag{1}$$

while the capacity that is overheard by the eavesdropper is

$$\gamma_e^{n_m} = \frac{W}{2}\log_2\left(1+\frac{P_0 h_{0,e}^{n_m}}{\sigma^2}\right), \tag{2}$$

then the secrecy capacity of m with no friendly jammer is

$$R_m(\{m\}) = \left[\gamma_m^{n_m} - \gamma_e^{n_m}\right]^+, \tag{3}$$

where $[x]^+$ represents $\max(0,x)$. When the data rate received by the eavesdropper is higher than that of the MUE m, all the information will be wiretapped, resulting in a zero secrecy capacity. $\{m\}$ is the coalition that MUE m belongs to and in the initial non-cooperative condition, MUE m lies in a singleton coalition which is formed by itself.

Assuming that the SBS k is transmitting on subchannel n_k, its capacity can be given as

$$R_k(\{k\}) = \frac{W}{2}\log_2\left(1+\frac{P_{\text{sbs}} h_{k,v_k}^{n_k}}{\sigma^2+\sum_{i\in I(n_k), i\neq k} P_i^{n_k} h_{i,v_k}^{n_k}}\right), \tag{4}$$

where $i \in I(n_k), i \neq k$, is the set of SBSs that interfere with k.

2.2 Friendly jammer

The SBSs are allowed to choose one MUE m as its client user to allocate a certain proportion of its power to transmit the noise for friendly jamming. The transmission power of the jammers imposes extra interference on the wiretap channel, exacerbating the eavesdropper's capacity on subchannel n_m and thus improves the secrecy capacity of corresponding MUE. We consider a scenario where the MUE and its jammers form a coalition, as described in Fig. 1.

Let $\boldsymbol{J}(m)$ denote the set of SBSs providing jamming power for MUE m, the corresponding coalition can be then indicated by $S = \{m, \boldsymbol{J}(m)\}$. After the help of jammers, the capacity of MUE m and that overheard by eavesdropper can be respectively presented as

$$\gamma_m^{n_m}(S) = \frac{W}{2}\log_2\left(1+\frac{P_0 h_{0,m}^{n_m}}{\sigma^2+\sum_{j\in J(m)} \alpha P_{sbs} h_{j,m}^{n_m}}\right), \tag{5}$$

$$\gamma_e^{n_m}(S) = \frac{W}{2}\log_2\left(1+\frac{P_0 h_{0,e}^{n_m}}{\sigma^2+\sum_{j\in J(m)} \alpha P_{sbs} h_{j,e}^{n_m}}\right), \tag{6}$$

where $\alpha \in (0,1)$ is the percentage of power an SBS allocates to friendly jamming. Then, the secrecy capacity of MUE m is

$$R_m(S) = \left[\gamma_m^{n_m}(S) - \gamma_e^{n_m}(S)\right]^+. \tag{7}$$

Note that the interference direct to the eavesdropper will also affect the communication between MUE and MBS. Friendly jammer makes use of the disparate value of interference that a jammer brings to the eavesdropper and the MUE to increase the secrecy capacity. Only if a jammer causes more interference to the eavesdropper than to MUE m can it possibly play a positive role and, in other words, have the qualification of being MUE m's jammer.

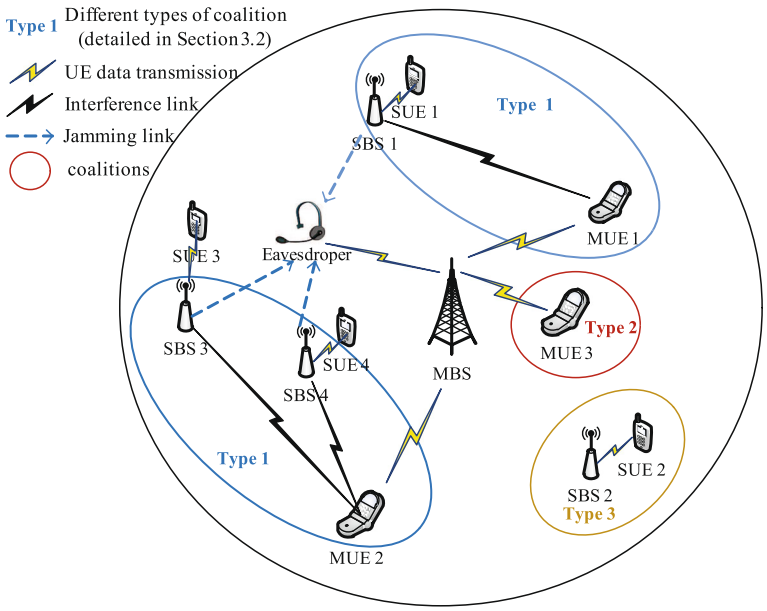

Fig. 1 An illustration of friendly jammer and coalition. When an SBS decides to be a jammer and designates a client MUE, it allocates a fraction of its total power to jam on the corresponding subchannel. The MUE and its jammers constitutes a win-win coalition

Proposition 1 *The necessary condition that SBS k is able to improve MUE m's secrecy capacity is that the channel gain between SBS k and MUE m is less than that from SBS k to the eavesdropper, i.e.* $h_{k,e}^{n_m} > h_{k,m}^{n_m}$.

A similar conclusion is drawn in [20], but we will proof it in a more mathematical way.

Proof Consider the high SINR scenario, the data rate of MUE and eavesdropper can be approximated as $\log_2\left(P_0 h_{0,m}^{n_m}/\sigma^2\right)$ and $\log_2\left(P_0 h_{0,e}^{n_m}/\sigma^2\right)$, respectively. Then, the secrecy capacity of MUE m can be given as

$$\begin{aligned} R_m(\{m\}) &\approx \left[\log_2 \frac{P_0 h_{0,m}^{n_m}}{\sigma^2} - \log_2 \frac{P_0 h_{0,e}^{n_m}}{\sigma^2}\right]^+ \\ &= \left[\log_2 \frac{h_{0,m}^{n_m}}{h_{0,e}^{n_m}}\right]^+. \end{aligned} \tag{8}$$

When SBS k comes to assist the secret communication, the increment of the secrecy capacity is

$$\begin{aligned} \Delta R_m &= R_m(\{m,k\}) - R_m(\{m\}) \\ &\approx \left[\log_2 \frac{P_0 h_{0,m}^{n_m}}{\sigma^2 + \alpha P_{\text{sbs}} h_{k,m}^{n_m}} \right. \\ &\quad \left. - \log_2 \frac{P_0 h_{0,e}^{n_m}}{\sigma^2 + \alpha P_{\text{sbs}} h_{k,e}^{n_m}}\right]^+ - \left[\log_2 \frac{h_{0,m}^{n_m}}{h_{0,e}^{n_m}}\right]^+. \end{aligned} \tag{9}$$

The problem can be divided into two cases according to the initial secrecy capacity of the MUE.

I. MUE m originally has a non-zero secrecy capacity.

In this case, we have $h_{0,m}^{n_m}/h_{0,e}^{n_m} > 1$. Only when (10) is satisfied can SBS k generate a positive increment in R_m.

$$\log_2 \frac{P_0 h_{0,m}^{n_m}}{\sigma^2 + \alpha P_{\text{sbs}} h_{k,m}^{n_m}} - \log_2 \frac{P_0 h_{0,e}^{n_m}}{\sigma^2 + \alpha P_{\text{sbs}} h_{k,e}^{n_m}} - \log_2 \frac{h_{0,m}^{n_m}}{h_{0,e}^{n_m}} > 0. \tag{10}$$

It can be easily obtained that $\left(\sigma^2 + \alpha P_k h_{k,e}^{n_m}\right) / \left(\sigma^2 + \alpha P_k h_{k,m}^{n_m}\right) > 1$, i.e., $h_{k,e}^{n_m} > h_{k,m}^{n_m}$.

II. MUE m has a zero secrecy capacity in the beginning.

In this case, $h_{0,m}^{n_m}/h_{0,e}^{n_m} \leq 1$ stands. Then, if (11) is satisfied, a positive increment in R_m can be guaranteed.

$$\log_2 \frac{P_0 h_{0,m}^{n_m}}{\sigma^2 + \alpha P_{\text{sbs}} h_{k,m}^{n_m}} - \log_2 \frac{P_0 h_{0,e}^{n_m}}{\sigma^2 + \alpha P_{\text{sbs}} h_{k,e}^{n_m}} > 0. \tag{11}$$

From (11) we can obtain

$$\left(h_{0,e}^{n_m} - h_{0,m}^{n_m}\right)\sigma^2 / \left(\alpha P_{\text{sbs}}\right) < h_{0,m}^{n_m} h_{k,e}^{n_m} - h_{0,e}^{n_m} h_{k,m}^{n_m}, \tag{12}$$

and because

$$\begin{aligned} 0 &< \left(h_{0,e}^{n_m} - h_{0,m}^{n_m}\right)\sigma^2 / \left(\alpha P_{sbs}\right) \\ &< h_{0,m}^{n_m} h_{k,e}^{n_m} - h_{0,e}^{n_m} h_{k,m}^{n_m} < h_{0,m}^{n_m}\left(h_{k,e}^{n_m} - h_{k,m}^{n_m}\right), \end{aligned} \tag{13}$$

the condition $h_{k,e}^{n_m} > h_{k,m}^{n_m}$ holds. □

Based on Proposition 1, one understands that only a fraction of SBSs are qualified to enhance the secrecy capacity of a certain MUE. We assume that every MUE can select one or more jammers on its eligible jammer list, while the SBS can only choose to serve one MUE. The rationale behind this is that the SBS concerns most about its own traffic and has to guarantee the performance of its own SUE v_k. It is injudicious to utilize much of its energy to protect the security of macro-layer, putting its own user at a reduced performance.

To compensate SBS k ($k \in \boldsymbol{J}(m)$) for its jamming power, MUE m buys the jamming power from its jamming SBSs as the monetary reward. The price ρ_k for unit power is defined as the marginal gain of SBS k in $\boldsymbol{J}(m)$, expressed as

$$\rho_k = \Delta R_m^k = R_m(S) - R_m(S\backslash\{k\}), \tag{14}$$

where S is the coalition that consists of MUE m and its current jammers, i.e., $S = \{m, \boldsymbol{J}(m)\}$, while $S\backslash\{k\}$ means eliminating element k from set S. The marginal gain, denoted by ΔR_m^k, is the increment of secrecy capacity that SBS k brings to MUE m when it joins this coalition. The total cost of MUE m is

$$C_m(S) = \sum\nolimits_{k\in\boldsymbol{J}(m)} \rho_k P_k^{n_m} = \alpha P_{\text{sbs}} \sum\nolimits_{k\in\boldsymbol{J}(m)} \rho_k. \tag{15}$$

2.3 Stage combined spectrum leasing

Besides the monetary reward, the MUEs also provide a resource reward to further encourage the SBSs to cooperate and guarantee their performance. This can be done through spectrum leasing. In classical spectrum leasing as discussed in [22, 30], MUE preserves a fraction β ($0 < \beta \leqslant 1$) of its superframe for the secret communication and leaves the remaining fraction $1 - \beta$ of the superframe for jammer's transmission. In this way, the working process can be divided into two stages, as illustrated in Fig. 2a. In the first stage, MUE communicates with the MBS, aided by its jammers. The jammers, in the meantime, transmit Gaussian noise to serve the MUE, disturbing the eavesdropper. In the second stage, MUE suspends its transmission and delegates the remnant of superframe to the jammers as the resource compensation. The jammers then can have free access to extra time and frequency resource to serve their own data.

In SCSL, as shown in Fig. 2b, β always equals to one, resulting in the merge of the first and the second stage, which means the serving and rewarding phases are allowed to work simultaneously. In this context, MUE m will communicate with MBS in the whole superframe

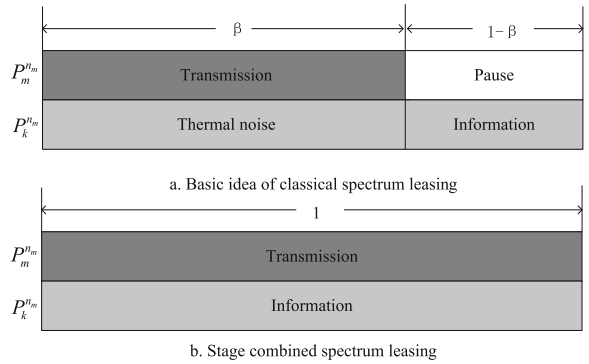

Fig. 2 A brief comparison between classical and stage combined spectrum leasing. $P_m^{n_m}$ and $P_k^{n_m}$ denote the transmission power of MUE m and jammer SBS k on channel n_m, respectively. The words illustrate the operations of MUEs and SBSs in the corresponding stage while the shades of each box intuitively show the signal strength, e.g., the *white box* in **a** means a zero power

period while the jammers transmit their own data, instead of the Gaussian noise, in the superframe. Note that the core of SCSL is the conventional Gaussian noise being replaced by the jammers' own useful data as the jamming signal. Due to the disability of MUE to decode the jammers' signal, the jamming power will also introduce interference to the MUE, no matter what type of jamming signal the jammers use. Hence, there is no difference between Gaussian noise and other data from MUE's perspective. This also applies to the eavesdropper. In this situation, the SBSs are able to transmit on an additional subchannel that belongs to the macro-layer, without harming the jamming performance. Since the jammers already obtain the resource in the beginning of the superframe (i.e., has already utilized the period β indicated in Fig. 2a), the MUE has no need to pause the transmission to give way for the jammers and thus saves the cost of performance loss in the second stage compared with classical spectrum leasing. In this way, the SCSL not only achieves the primary goal of friendly jamming but also grants more resources (time or frequency) to the jammers and MUE, allowing a performance improvement for both jammers and MUE compared with the classical spectrum leasing. By ensuring the performance of SBSs in the jamming period, the SCSL is a much stronger incentive mechanism for SBSs to cooperate. In SCSL, the throughput of an SBS that serves MUE m in coalition S is

$$R_k(S) = \frac{W}{2}\left[\log_2\left(1+\frac{(1-\alpha)P_{\text{sbs}}h_{k,v_k}^{n_k}}{\sigma^2+\sum_{i\in I(n_k)}P_i^{n_k}h_{i,v_k}^{n_k}}\right) + \log_2\left(1+\frac{\alpha P_{\text{sbs}}h_{k,v_k}^{n_m}}{\sigma^2+P_0h_{0,v_k}^{n_m}+\sum_{j\in J(m)}\alpha P_{\text{sbs}}h_{j,v_k}^{n_m}}\right)\right], \tag{16}$$

where $P_i^{n_k}$ is the transmission power of SBS i that interferes the SBS k on subchannel n_k. When i is a jammer, a proportion α of its power is allocated to the wiretap channel. Otherwise, it would transmit at full power on its original subchannel n_k. Consequently, we have

$$P_i^{n_k} = \begin{cases} P_{sbs} & i \text{ is not a jammer,} \\ (1-\alpha)P_{sbs} & i \text{ is a jammer.} \end{cases} \tag{17}$$

2.4 Two-way selection as an optimization problem

As we see, the MUE and its cooperated jammers as a coalition S, all the coalitions (including the singleton coalitions, i.e., an MUE without a jammer or a non-jammer SBS) in a network form a network partition $\prod = \{S_1, S_2, \ldots\}$ whose formal definition will be given in next section. The ultimate goal of this work is to find the best partition $\prod$ that could optimize the secrecy capacity of the MUEs while guarantee a good performance of the SBSs. The problem can be formulated as

$$\max_{\Pi} \sum_{m\in\mathbb{M}} R_m + \sum_{k\in\mathbb{K}} R_k, \tag{18}$$

where R_m denotes the secrecy capacity of MUE m and accrodingly, R_k is the capacity of SBS k, which are defined in (7) and (16), respectively.

Nevertheless, the huge number of communication nodes in UNDs makes it almost impossible to solve the above problem in a centralized method due to the enormous network information to collect as well as the astounding computational complexity. The likely number of $\prod$ is given by the Bell Number which has reached to 115975 when there's only 10 nodes in the network. Hence, we turn to the distributed and practical methods and model the problem as the a coalition formation game to be detailed in the next section.

3 Coalitional game

In this section, we model the two-way selection problem between MUEs and SBSs as the coalition formation game in partition form with non-transferable utility (NTU). Through the game, the players choose the best allies to maximize their utilities in a distributed manner, the result of which satisfies the Nash stability and individual stability.

3.1 Game formulation

The coalitional game theory provides a convenient analytical tool for studying the interaction among the players to form the cooperative groups, and it has been applied to wireless communication system in many articles [28–31]. To further explain the concept of coalition formation game in partition form, we first introduce the definition of the coalition partition [32].

Definition 1 *A coalition partition or coalitional structure is defined as the set* $\prod_{\Omega} = \{S_1, S_2, \ldots, S_L\}$ *which partitions the player set* Ω *(in our game* Ω *is the collection of all MUEs and SBSs, in other words,* $\Omega = \mathbb{M} \cup \mathbb{K}$*), i.e.,* $\forall k, S_k \subseteq \Omega$ *are disjoint coalitions such that* $\bigcup_{l=1}^{L} S_l = \Omega$.

The coalition formation game in partition form is introduced in [33] as a class of game in which the profit of a coalition S, and its members have a strong dependence on the coalition partition and the way that the player in $\Omega \backslash S$ is organized. The coalitional game in partition form with NTU can be defined as follows [34]:

Definition 2 *A coalitional game in partition form with NTU is defined by a pair* (Ω, U)*, where* Ω *is the set of players while* U *is a partition function that maps any coalition* $S_l \subset \Omega, S_l \in \Pi_{\Omega}$ *to a closed convex subset of* $\mathbb{R}^{|S_l|}$. $U(\Pi_{\Omega}, S_l)$ *is the payoff vector for every player in* S_l.

In the proposed game, the performance of the members in any coalition S_l is affected by the coalitional structure of the players outside the S_l. Hence, it has the following property:

Property 1 *The game between the MUEs and SBSs is indeed in partition form.*

For example, if an SBS k decides to act as a jammer after evaluating the trade-offs and merges into a coalition S which contains MUE m, a fraction of its power will be transferred to the subchannel n_m, attenuating the co-layer interference on subchannel n_k suffered by the SBSs outside S. As a result, the performance of a player is closely related to the organization of players from other distinct coalitions and has a dependence on the network structure.

As is discussed above, for a given structure $\prod_{\Omega} = \{S_1, S_2, \ldots, S_L\}$, the player's utility in S_l is defined by the utility function U which has the form of

$$U(\Pi, S_l) = \left\{ \mathbf{u} \in \mathbb{R}^{|S_l|} | u_i(\Pi, S_l), i \in S_l \right\}. \tag{19}$$

In this game, there are two types of the players, i.e., MUEs and SBSs, which have different goals as well as cost functions to form the coalition. Therefore, we formulate two kinds of utility functions respectively to measure the income of MUEs and SBSs. In the first place, for MUE $m \in \mathbb{M}$, the utility in coalition $S \in \Pi, m \in S$ is defined as

$$u_m(\Pi, S) = \begin{cases} -\infty, & |S \cap \mathbb{M}| > 1 \text{ or } S \in h(m), \\ R_m(\{m\}), & |S| = 1, \\ R_m(S) - C_m(S), & \text{otherwise}, \end{cases} \tag{20}$$

where $h(m)$ is the record of the historical coalitions that m has been to. The players are not permitted to revisit the coalition that they had left previously and will acquire a negative infinite utility if they do so. This rule is adopted by many studies [28, 29, 31] as an effective measure to guarantee a faster convergence of the algorithm. Note that the singleton coalition $\{m\}$ will never be recorded since a player is allowed to quit a coalition whenever it discovers that it is better to be single. In (20), Π is the current partition while S is the coalition that MUE m belongs to. $R_m(S)$ is given by (7) and represents the secrecy capacity that MUE m obtains with the help of the jammers in S. $C_m(S)$ is the total cost for the jamming power which is defined in (15).

The main rationale behind the utility function u_m is that in the proposed scheme, the purpose of an MUE to join the game is to find the jammers who are keen on supporting its secret communication, making up a coalition in which the jammers have the right to send messages on the MUE's channel in a relatively low power. Henceforth, we summarize the two features of a legal coalition which contains the MUE m. First, a non-singleton coalition is formed by the MUE m and its jammers only. Second, all the members in the coalition transmit on the subchannel n_m with full (for MUE m) or a portion (for jammers, if there's any) of their power. In the condition that $|S \cap \mathbb{M}| > 1$, more than one MUE exists in the coalition S, violating the two features above. The reasons are as follows. Firstly, due to the fact that merely the SBSs have the function of jamming, such a coalition can only be formed by *one* MUE and several SBSs. The first rule is broken by adding additional MUEs into the coalition since the MUE cannot be a friendly jammer of another MUE. Secondly, each MUE in the system occupies a different subchannel so that no interference exists within the macro-layer. If there are some MUEs other than MUE m that stay in the coalition, the extra MUEs are working on subchannels distinct from that of MUE m's and are banned to transmit on subchannel n_m, which conflicts the second feature. From what has been discussed, we set a negative benefit of forming a coalition with another MUE to prevent such event. For the case that a legal coalition is formed, the goal of MUE m is to pay less for better secret transmission via carefully selecting its allies among the potential jammers. When there is only one MUE m in S, i.e., $|S| = 1$, with no assist of any SBS, it has no need to pay for the jamming power. The utility of m is simply its secrecy capacity in this case. Under the circumstances that at least one jammer comes to help, the profit of m is the secrecy performance minus the expense.

For SBS $k \in \mathbb{K}$, the utility in coalition $S \in \Pi, k \in S$ is defined as

$$u_k(\Pi, S) = \begin{cases} -\infty, & |S \cap \mathbb{M}| = 0 \,\&\, |S| > 1 \text{ or } \rho_k < 0 \text{ or } S \in h(k), \\ R_k(\{k\}), & |S| = 1, \\ R_k(S) + \alpha P_{\text{sbs}} \rho_k, & \text{otherwise}, \end{cases} \tag{21}$$

where ρ_k, given in (14), is the monetary emolument for unit jamming power payed by client MUE. Similar to $h(m)$, $h(k)$ is the historical record of the coalitions that SBS k has once joined in. $R_k(\{k\})$ and $R_k(S)$ are given by (4) and (16), respectively, as the capacity of SBS k in different situations.

Similar to MUE players, the utility function of SBSs includes their capacity and the money they receive (if any), as presented in the last two lines of (21), when they form a legal coalition. There are also some coalitions considered as illegal. When $|S \cap \mathbb{M}| = 0$ and $|S| > 1$ holds, all members in S are SBSs, in other words, jammers, which makes no sense due to the absence of an MUE. The impetus for an SBS to assist the secret communication of the macro-layer is money and resource incentive that lead to the boost of both performance and income. As is analyzed, a non-singleton coalition is supposed to have one MUE that needs friendly jamming and takes the role of offering the bonus to SBSs. Consequently, there is no inspiration for an SBS to participate in a group without MUE. The utility of merging into a coalition with pure SBSs is thus set to negative infinite, showing that it is extremely unwise to do so. Other than the unit price of jamming power, ρ_k also presents the marginal gain of the secrecy capacity that SBS k brings to its client MUE. The sign of ρ_k represents the impact of SBS k on its client MUE in the presence of the other jammers in the coalition. A positive ρ_k implies that the existence of SBS k is meaningful since k indeed elevates the MUE's secrecy performance. On the contrary, a negative ρ_k means that the client MUE would have a higher secrecy capacity without SBS k. As the paramount goal of this game is to protect the macro-layer's information from the malicious eavesdropper, any collaborator that may impair the MUE's secrecy capacity will be declined and eliminated since it no longer performs as an effective jammer. The profit is set to negative in virtue of the MUE's rejection of cooperation, compelling SBS k to split from the coalition.

From the description of utility function we can clearly see that it is an individual performance measurement that cannot be transferred among the MUEs and SBSs, showing the NTU property of the game.

Now that the individual revenue is well defined via the utility function U, the utility of a coalition $S \in \Omega$ in partition Π can then be set as the sum of all its members' profit, i.e.,

$$\theta(S) = \sum\nolimits_{k \in S} u_k(\Pi, S). \tag{22}$$

Note that $\theta(S)$ also means the entire capacity (for SBSs) and secrecy capacity (for MUEs) coalition S achieves.

Property 2 *The proposed coalition formation game* (Ω, U) *is non-superadditive.*

To address property 2, consider two disjoint coalitions $S_1, S_2 \in \Omega$, each of which contains only one MUE with non-zero secrecy capacity, i.e., $\theta(S_1) > 0$, $\theta(S_2) > 0$. Then, as defined in (20) and (22), the merging coalition $S_1 \cup S_2$ would have a zero payoff because of the co-existence of two MUEs. Thus, we have

$$\theta(S_1 \cup S_2) = 0 \leq \theta(S_1) + \theta(S_2). \tag{23}$$

Therefore, this game does not meet the nature of superadditive.

Property 3 *The grand coalition which consists of all the players will never form in the proposed game.*

This property is obvious due to the nature of non-superadditive.

3.2 The algorithm and distributed implementation

Up to now, we have modeled the two-way selection problem between MUEs and SBSs as coalition formation game in partition form. This type of game is comprehensive to solve but can capture the inter-coalition effects in many realistic situations [30, 35]. In this section, we develop a decentralized algorithm to endow the players with the capability of automatically finding their best collaborators in terms of the network environment, applying the merge-and-split method [36].

The basic idea of merge-and-split is that the player gradually improves its performance by constantly comparing the utility in different coalitions and switch to a superior one through the action of merging into or splitting from a coalition, until it reaches the point that the utility cannot be further increased. To decide which coalition is better, i.e., which coalition the player prefers to be a member of, we introduce the preference relation [29], $\succeq_i$, for any player $i \in \Omega$ to denote player i's preference between two different coalitions $S_1 \subseteq \Omega$ with $i \in S_1$ and $S_2 \subseteq \Omega$ with $i \in S_2$. For example, $S_1 \succeq_i S_2$ implies that the player i is more inclined to join coalition S_1 than S_2 or at least it prefers indifferently, while the asymmetric counterpart, $S_1 \succ_i S_2$, means that player i strictly prefers to be a member of S_1. Here, we define the preference relation according to the individual payoff:

$$S_1 \succeq_i S_2 \Leftrightarrow u_i(\Pi_1, S_1) \geq u_i(\Pi_2, S_2), \tag{24}$$

where S_1, S_2 are two different coalitions potentially joined by player i. Π_1 and Π_2 are the initial partition and the new partition after player i switching to S_2, respectively. Based on this preference order, we define the following switching rule for coalition formation:

Definition 3 *Given a partition* $\Pi_1 = \{S_1, S_2, \ldots, S_L\}$ *of the player set* Ω*, player* $i \in \Omega$ *decides to split from its*

current coalition S_l, $l \in 1, 2, \ldots, L$ *to join another coalition* $S_m = \Pi_1 \cup \{\emptyset\}$, $S_m \neq S_l$ *if and only if* $S_m \cup \{i\} \succ_i S_l$. *After switching,* Π_1 *is modified into a new partition* $\Pi_2 = (\Pi_1 \backslash \{S_m, S_l\}) \cup (S_l \backslash \{i\}, S_m \cup \{i\})$.

The switching rule establishes the principle for players in the coalition formation process. At any moment a player discovers a coalition that can strictly improve its income, it will leave the current coalition and participate in the new one. By repeating the switching operation, the players are able to ameliorate their performance step by step until the network becomes stable. From what has been presented above, we can observe that the players leave the low-paying coalition and switch to a high-paying one, regardless of the effect on other members except the MUE. Hence, in the proposed game, the players adopt a relatively selfish strategy to maximize their own benefits rather than an altruistic one. Moreover, whenever a player i makes a move, it needs to update the historical record $h(i)$, adding the coalition that it newly leaves to the history set.

The basic process of classical merge-and-split algorithm using the switching rule described above is shown in Fig. 3. The players explore the possibility of performing a switching operation. In the proposed algorithm, we consider the players act in a greedy way, finding the most preferred coalition to join.

In each loop, in order to find the top preferred coalition, every player has to examine all the remaining coalitions, which is quite heavy workload and time-consuming for the player. From what can be seen in (20) and (21), an SBS will achieve no benefit joining a coalition composed of SBS-only and no two MUEs can coexist in the same coalition. As a result, there are only three possible types of coalitions in the final network structure: singleton coalitions with one MUE which cannot find a proper jammer; coalitions with one MUE and its jammers in which the MUE is chosen as the coalition-head, taking the role of negotiating with SBSs in and out of its coalition; and singleton coalitions with one SBS that is unwilling to provide jamming service or being rejected by its possible client MUEs. In this context, an SBS in the network only has to make a decision either trying to be some MUE's jammer or working alone, with no need to negotiate with other SBSs. As for MUEs, they can just negotiate with SBSs to see whether the collaboration is profitable for both sides. To further confine the possible negotiators, we use Proposition 1 in Section 2 to exclude the unqualified allies for both MUEs and SBSs. If SBS k is not able to improve MUE m's secrecy capacity, there is no need for them to

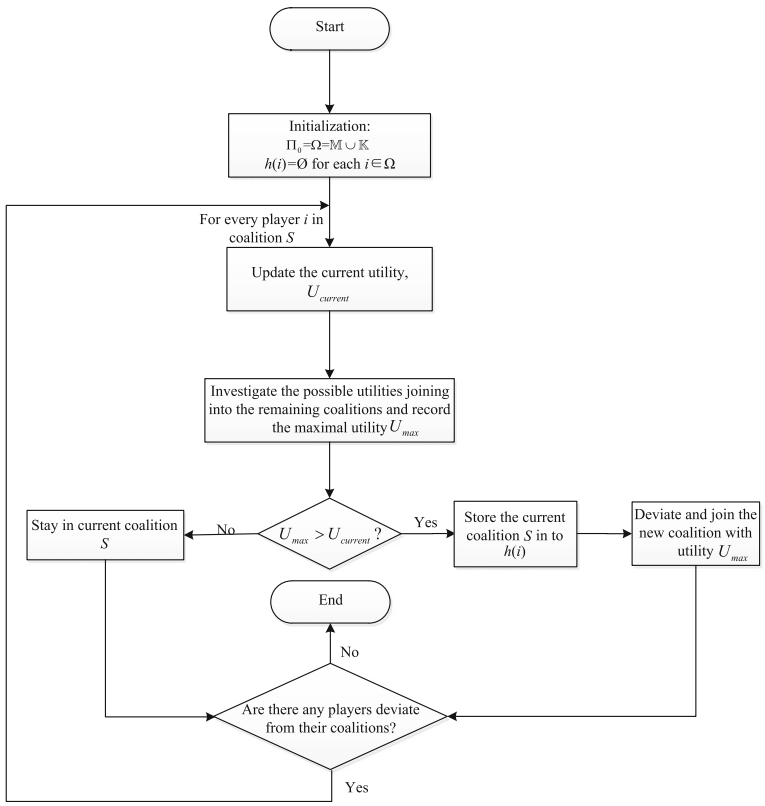

Fig. 3 An illustration of basic approach of merge-and-split

negotiate. In this case, SBS k has no necessity to consider the coalition that contains MUE m and vice versa. Thus, from an SBS's perspective for determining the switching operation, it simply negotiates with the MUEs sequentially on its partner list to see the possibility of switching. Similar to SBSs, an MUE negotiates with the SBSs on its list. The difference is that there is still space to further refine its potential partners. From an MUE's perspective, it only needs to consider about those SBSs whose coalition lies in the third class, i.e., singleton coalition with only an SBS. The reason for this is that an MUE has no benefit switching to a coalition that contains the MUE, ruling out the first two kinds of coalitions.

In summary, the predigested algorithm of two-way friendly jammer selection, shown in Table 1, can be divided into three phases: qualification confirmation, coalition formation, and friendly jamming. The network is initially partitioned by Ω, with all players that behave in a non-cooperate way. In the first stage, every player identifies its qualified coalitional partner through channel estimation. To start with, the SBSs estimate the channel gain to the eavesdropper as well as the MUEs in the network. Each SBS compares the channel gains and generates a partner list Ψ including the potential client MUEs in line with Proposition 1. The information of the channel gains are collected by MBS from each SBS and broadcasted to the MUEs. With the necessary channel information, each MUE can also filter out the incompetent jammers. In the second phase, each player investigates the possible switching operation among a refined collection of coalitions in the partner list. To compute the utility in a distributed manner, the solitary SBSs just calculate their capacities. From the jamming SBS's aspect, this can be done through negotiating with the coalition head. During this process, the MUE informs the SBS of the price ρ_k it provides according to (14) while the SBS estimates the capacity on this channel. In this implementation, ρ_k can be calculated using the channel gains broadcasted by MBS in the first stage. To save the storage, an MUE m only saves the necessary data such as $h_{k,e}^{n_m}$, where k is the SBS that lies in the partner list. As for the SBS, the capacity can be estimated via the feedbacks from its SUE v_k without much effort. For the convenience of MUEs to determine the SBSs that need to negotiate with, the SBS can keep a one-bit-label so that the MUE can tell whether it is alone or not. As for MUEs, the utility in (20) can be naturally found since all the required channel information is accessible. After the coalition formation, the SBSs start to jam for its client MUE. The proposed mechanism requires no centralized scheduler, and provides the players with the capability of independently comparing different coalitions as well as performing the switching operation.

Note that although we assume a full buffer traffic, the proposed game still works under the burst traffic scenario for that the coalition formation process needs not to be changed. The only difference is that an MUE needs to send a control message at the beginning as well as the end of the communication to its jammers so that the jammers could know when to start and finish their jamming service.

Table 1 Simplified coalition formation algorithm for two-way friendly jammer selection problem

Initialization

The coalitional structure is initialized as $\Pi_0 = \Omega = \mathbb{M} \cup \mathbb{K}$ and each player i's history set $h(i)$ is set empty.

Phase 1: Qualification Confirmation

a Each SBS k measures the channel gain to the eavesdropper and MUEs, i.e., $h_{k,e}^{n_m}, h_{k,m}^{n_m}, m \in \mathbb{M}$.
b MBS broadcasts the collected channel information to MUEs.
c Each player i calculates its potential partner list.
For SBS k, $\Psi_k = \{m | h_{k,e}^{n_m} / h_{k,m}^{n_m} > 1, m \in \mathbb{M}\}$,
For MUE m, $\Psi_m = \{k | h_{k,e}^{n_m} / h_{k,m}^{n_m} > 1, k \in \mathbb{K}\}$.

Phase 2: Coalition Formation

Loop:

Given the current partition $\Pi_{current}$ (in the beginning, $\Pi_{current} = \Pi_0$), for every player i in coalition $S \in \Pi_{current}$

a Update the utility in S, $U_{current} = u_k(\Pi_{current}, S)$
b For SBS, find the coalitions that contain the MUEs in Ψ_i,
$S_\Psi = \{S' | S' \in \Pi_{current} \backslash S, m \in \Psi_i, m \in S'\}$
For MUE, find the SBSs who are still alone in Ψ_i,
$S_\Psi = \{S' | k \in \Psi_i, k \in S', |S'| = 1\}$
c Investigate the possible switching operation among $S' \cup \{\emptyset\}$, according to the switching rule. Record the maximal utility U_{max} and the corresponding coalition
d *If* $U_{max} > U_{current}$
Player i stores the current coalition S into history set $h(i)$, and joins the new coalition
else
Player i stays in the current coalition and the coalition partition does not change
end

Until: No player deviate from its coalition.

Phase 3: Friendly Jamming

The SBS in non-singleton coalition allocates α of the total power on its client MUE m's subchannel n_m to transmit the information as the jamming noise. MUE pays to its jammers according to (14) and (15).

3.3 Convergence and stability

Convergence is of great importance in the research of coalition formation algorithm. The convergence of the proposed algorithm can be guaranteed, as follows.

Proposition 2 *From the initial state of the coalition partition, the convergence of the proposed coalition formation game is guaranteed.*

Proof With a certain number of players in the network, the number of partitions that can be formed is finite, given by the Bell number $B_{|\Omega|}$. As we regulate a negative payoff for players going back to the history coalitions in $h(i)$,

each deviation of the players leads to a new partition of the network. Since the number of the possible partitions is bounded, our algorithm surely converges in a finite number of iterations. □

To study the stability of the algorithm, we use the concepts of individually stable and Nash-stable from [32]:

Definition 4 *A partition* $\Pi = \{S_1, S_2, \ldots, S_L\}$ *is individually stable if there do not exist a player* $i \in \Omega, i \in S_l$ *and a coalition* $S_k \in \Pi \cup \{\emptyset\}$ *such that* $S_k \cup \{i\} \succ_i S_l$ *and* $S_k \cup \{i\} \succeq_j S_k, \forall j \in S_k$ *holds.*

Definition 5 *A partition* $\Pi = \{S_1, S_2, \ldots, S_L\}$ *is Nash-stable if* $\forall i \in \Omega, i \in S_l, S_l \succeq_i S_k \cup \{i\}$ *for all* $S_k \in \Pi \cup \{\emptyset\}$.

The relationship between the two stability concept is that a Nash-stable is individually stable [32]. From what can be seen, the Nash-stable is stronger than the individually stable. The essence of the Nash-stable is that in the final partition Π_f, no player can find a coalition that can further improve its payoff; thus, the player has no incentive to deviate from its current coalition.

Proposition 3 *The final partition* Π_f *resulted from the proposed coalition formation game is Nash-stable as well as individually stable.*

Proposition 3 is obvious and a similar proof can be found in [29] and [31].

The communication and computational complexity for a player to detect the switching operation in each loop is $O(K)$ (if it is an MUE) or $O(M)$ (if it is an SBS) in the worst case where all players behave in a non-cooperated way and any one of the SBSs has the qualification of staying on any MUE's potential partner list. In fact, the actual complexity is much less in realistic situation.

3.4 Adapting to the dynamic feature of wireless network

One distinctive nature of the wireless network is the ever changing environment which is caused by the time varying channel states, the mobility of the users, the plug-in feature of the SBSs, etc. Such changes observably modify the utilities of the players so that a reorganization of the network partition may be necessary in order to guarantee an optimal performance for all the SBSs and MUEs. Due to the abovementioned changes in the network, the proposed algorithm presented in Table 1 can be executed periodically as a response. According to our previous analyses, the algorithm is definite to converge within a finite number of steps because the possibility of switch operation is limited, no matter what the initial state is. Hence, the convergence and stability nature of the algorithm still hold, regardless of the variation of user's location as well as the randomness of the wireless channel. Note that the period of executing the proposed algorithm can be chosen according to the frequency of the changes in the network, which is beyond the scope of this paper.

4 Numerical results and discussions

In this section, we validate the efficacy of the proposed two-way selection algorithm for the coalitional game in UDNs. For simulation, we consider a macrocell with radius of 400 m where the MBS stands in the center, serving 10 MUEs. Unless otherwise stated, 80 small cells are deployed uniformly in the coverage of MBS, each of which has one active SUE. All users in the system, i.e., MUEs and SUEs occupy one subchannel. Furthermore, the channel model includes the large scale fading and Rayleigh fading which follows the exponential distribution with parameter 1 and the power of white noise is −174 dBm/Hz. The macro and small-cell layers are working on orthogonal sets of subchannels in the initial stage with 30 subchannels in total which are allocated to the small cells. The maximum values of power for MBS and SBS are configured as 46 and 23 dBm, respectively. The primary parameters utilized in the simulation are summarized in Table 2.

Note that each jammer SBS allocates a fraction, α, of its total power to jamming. In Fig. 4, we investigate the influence of jamming power factor α on the system performance. The result shows that the overall performance of either MUEs or SBSs has a remarkable improvement compared with the non-cooperative network structure. We also observe that the average secrecy capacity of MUEs does not have an evident change when α reaches 0.2. The reason is that, from Eqs. (7), (15), and (20), we can see that the utility of an MUE is not a monotone function of jamming power αP_{sbs} because the artificial interference exerted on eavesdropper will also play a side effect to MUEs accordingly. Hence, it is not the bigger the better in terms of the jamming power of SBS and there must exist an optimal value p^*. When the variable α rises, the MUE requires less SBS to obtain the jamming power that is approximate to p^*. As in the experiment, the average number of required jammers decreases from 2.2 when $\alpha = 5$ % to 1.8 at value $\alpha = 20$ % and at last to only 1.2 when $\alpha = 95$ %. No matter what value of α is, the

Table 2 Primary simulation parameters

Radius of MBS, R_m	400 m
Number of MUEs, M	10
Subchannels allocated to SBSs, N_m	30
Maximum power of MBS, P_m	46 dBm
Maximum power of SBS, P_{sbs}	23 dBm
Power of white noise, σ^2	−174 dBm/Hz
Bandwidth of an subchannel, W	180 kHz

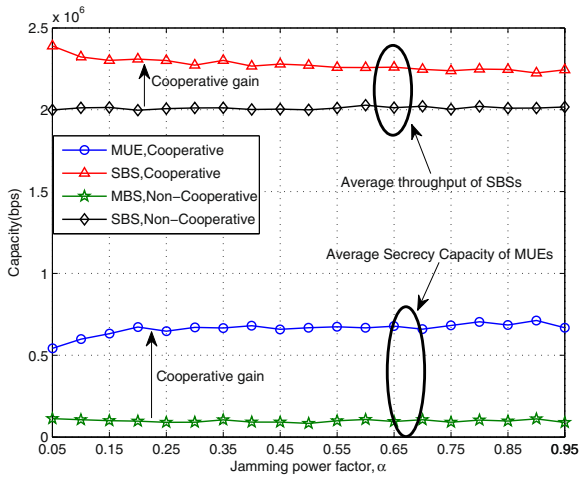

Fig. 4 The average secrecy capacity of MUEs and the average capacity of SBSs as a function of α

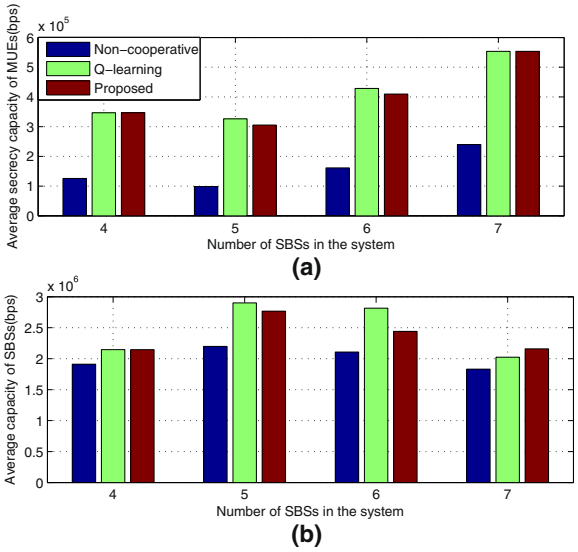

Fig. 5 A comparison of average secrecy capacity of MUEs and average capacity of SBSs under Q-learning and the propose mechanism. (M=3)

average secrecy capactity will not have a severe fluctuation because of the automated accommodation of the actual jammers in our final network structure. This indicates that the jamming power has a relatively weak impact on system performance compared with that of the network structure. For this aspect, we can choose a fixed α to reduce the complexity of the algorithm and focus on the process of coalition formation. In the following experiment, we set $\alpha = 0.2$. The joint optimization of the network structure together with the resource allocation, say power optimization, will be our future work to explore.

We first compare the proposed coalitional game with the friend-or-foe Q-learning [37] (referred to as FFQ below) in a relatively small scale network, the result of which is provided in Fig. 5. From what can be seen, the proposed game has a close outcome as FFQ learning in terms of both average secrecy capacity of macrocell layer and average capacity of small-cell layer and it may even reach the performance of FFQ in some situations. Since in FFQ, the SBSs take the learning process to estimate the Q values of jamming for each MUE, the size of the action set for a certain player i is $M+1$, including stand alone and actively jam for some MUE. Assuming that there are T states, then the total number of tuples $< s, a_1, a_2, \ldots >$ (where s denotes the state of a game and a_i denotes the action of the player i) will be $T \times (M+1)^K$. The basic idea of Q-learning algorithms is to visit the tuple $< s, a_1, a_2, \ldots >$ infinitely often so that the Q value $Q(s, a_1, a_2, \ldots)$ will converge to $Q*$ which reveals the real payoff of the players. This means that far more than $(M+1)^K$ loops are needed before the learning procedure terminates. Furthermore, in order to store and update all the elements $Q(s, a_1, \ldots, a_K)$ in a Q table, the space complexity is also $O((M+1)^K)$; hence, the requested memory grows exponentially as the MUE and SBS increase. So, it appears that the Q-learning is space-and-time-consuming that may restrain the practical application in large scale scenarios. While in coalition formation stage, the final network structure can usually be found with a maximal number of 3 loops. In Section 3.3, we have analyzed that the computational complexity in each loop is $O(K)$ (for MUEs) or $O(M)$ (for SBSs) in the worst case; hence, the overall complexity in consideration of all players is $O(MK)$ within one loop. Therefore, we can find that the coalitional game is able to find a feasible solution that is not much worse than FFQ with a far smaller cost in terms of time and space complexity.

Figure 6 and Table 3 display the proposed algorithm's ability of enhancing MUE's secrecy capacity. Figure 6 illustrates the secrecy capacity of each MUE before and after coalition formation in one snapshot. From what can be observed, in the initial stage when players behave in a non-cooperative manner, only 4 MUEs achieve a non-zero, yet very low secrecy capacity. We denote the set of MUEs that naturally have a positive secrecy capacity by Ξ_m. According to our simulation result, the mean size of Ξ_m is 3.88, indicating that more than half of MUEs are completely exposed to the eavesdropper. This can be an appalling conclusion that most of the users would be in extreme danger once an eavesdropper is installed in the network. By cooperating with the SBSs, as depicted in Table 3, the average number of MUEs that have non-zero secrecy capacity rises to 9.76. This means that our cooperative partition can protect almost every MUE well in the network, which is also verified in Fig. 6. Furthermore, the average performance of MUEs in Ξ_m is doubled by applying the proposed algorithm. At the same time,

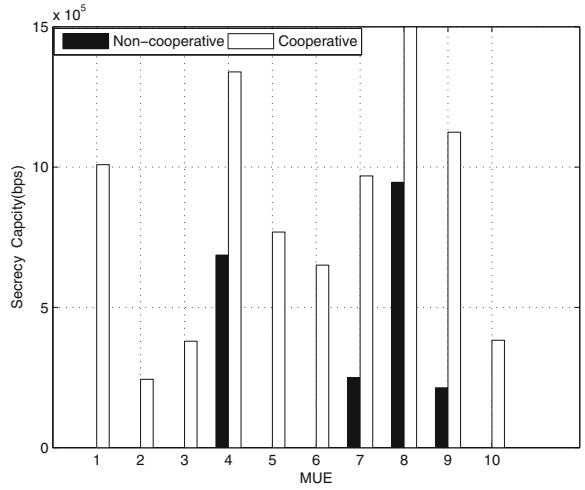

Fig. 6 The secrecy capacity of each MUE before and after coalition formation in one snapshot. Note that in cases 1, 2, 3, 5, 6, and 10, the secrecy capacity values are zero

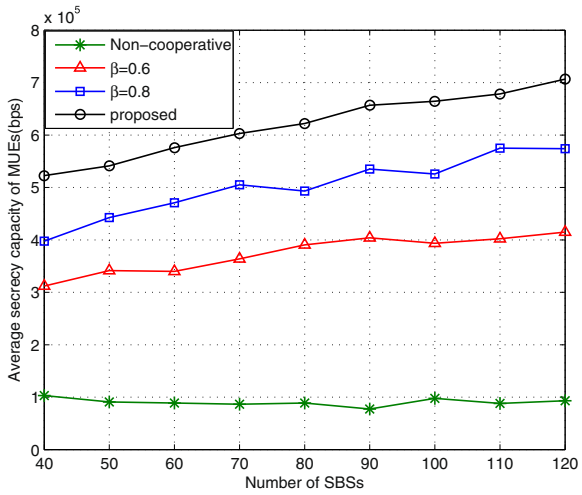

Fig. 7 Average secrecy capacity of MUEs under the proposed friendly jamming mechanism and under the traditional spectrum leasing scheme with different β values when the number of SBSs increases

the small-cell layer can also acquire a 16.92 % gain of the capacity. To summarize, the proposed two-way selection friendly jamming scheme effectively increases the resistance to the eavesdropper and is advantageous to both MUEs and small cells.

In Figs. 7 and 8, we illustrate the performance of the MUEs and SBSs under the spectrum leasing and the proposed SCSL scheme, as a function of the number of SBSs. The average secrecy capacity of MUEs increases with a rising β while the capacity of SBSs decreases. In spectrum leasing, the jammers use thermal noise as jamming signal in first fraction β of the superframe and obtain the remaining $1-\beta$ as resource bonus. Actually β is a parameter that controls the resource distribution between the client MUE and its jammers. The larger the β, the more resource the MUE maintains and the less incentive the jammers obtain. Hence, the tendencies of the average capacity of MUEs and SBSs have an opposite trend when β changes. On the contrary, for either MUE or SBS, the proposed SCSL mechanism can always guarantee a better performance than the basic spectrum leasing, regardless of the parameter values. In consistent with the analysis in Section 2, the SCSL saves energy as well as time compared with noise transmission in SBSs, and it also removes the idle time for MUE, making a more efficient use of the precious communication resource.

Figure 7 also shows the impact of the number of SBSs on the secrecy capacity of MUEs. Firstly, we can see that the MUEs have a poor secrecy performance in non-cooperative condition, i.e., lower than 100 kbps. In addition, the original secrecy capacity is not influenced when the quantity of SBSs increases. The reason is that

Table 3 Performance comparison between cooperative and non-cooperative system ($M=10$, K=80)

Parameters	Non-cooperative	Cooperative	Gain (%)
Mean number of MUEs that have positive SC[a]	3.88	9.76	151.55
Mean SC of MUE(bps)	9.35×10^4	6.09×10^5	551.34
Mean SC of MUEs in Ξ_m(bps)	2.43×10^5	7.55×10^5	210.70
Mean Capacity of SBS(bps)	2.01×10^6	2.35×10^6	16.92

[a]We use SC to represent secrecy capacity in this table

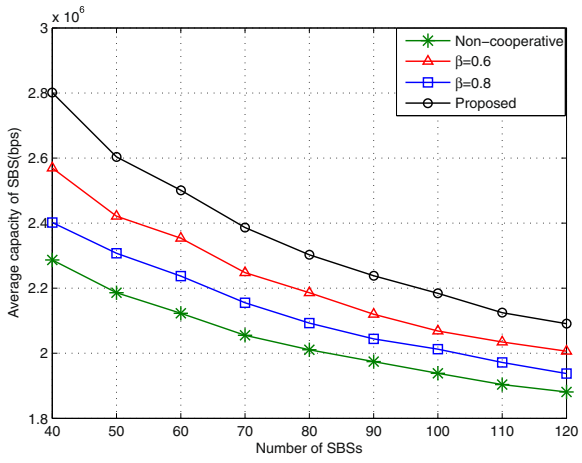

Fig. 8 SBSs' capacity under the proposed friendly jamming mechanism and under the traditional spectrum leasing scheme with different β values when the number of SBSs increases

in non-cooperative scenario, the two layers work on the orthogonal sets of frequencies that would not affect each other. Hence, the MUEs' performance is independent of the small cells in the system and stays essentially constant as the number of the SBSs increases. However, the secrecy capacity in the proposed scheme is highly correlated to the number of SBSs in the system. We can observe an obvious enhancement of secrecy capacity along with the augment of small cells. The average secrecy capacity of MUEs improves by 35.17 % as the number of SBSs increases from 40 to 120. The reason is that the larger number of SBSs gives a wider choice of candidate jammers, making it easier for MUEs to select proper jammers. Additionally, according to Proposition 1, the SBSs locating around the eavesdropper have more impact on disturbing and can thus better protect the MUE's privacy. Consequently, those SBSs become the competitive focus of the MUEs. When there are not many small cells, the quantity of such SBSs that can provide high quality of jamming service is relatively small. As the number of SBSs gradually rises, the density of the small cells grows, resulting in a larger amount of SBSs that lie in the vicinity of the eavesdropper. Besides the capable jammers, the ordinary jammers on the MUE's potential partner list will also increase, providing a higher possibility to find the SBSs that are willing to cooperate.

In order to analyze how this friendly jammer scheme affects the SBSs in the system, we measure the increment of the capacity of the SBSs. Fig. 9 shows the average SBSs' capacity gain after applying the scheme. Moreover, we divide the SBSs into two classes—jammers and non-jammers—according to the role that they play. The performance of the two classes of SBSs is counted separately and is also displayed in Fig. 9. Similar to what has been demonstrated in Table 3, the average capacity

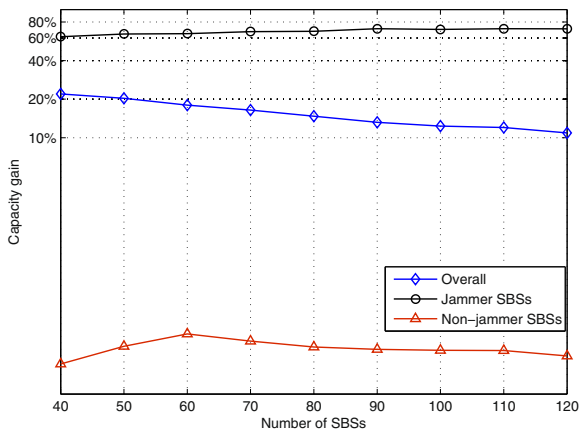

Fig. 9 The average capacity gain of the jammer SBS, non-jammer SBS, and overall SBSs when the friendly jamming approach is applied

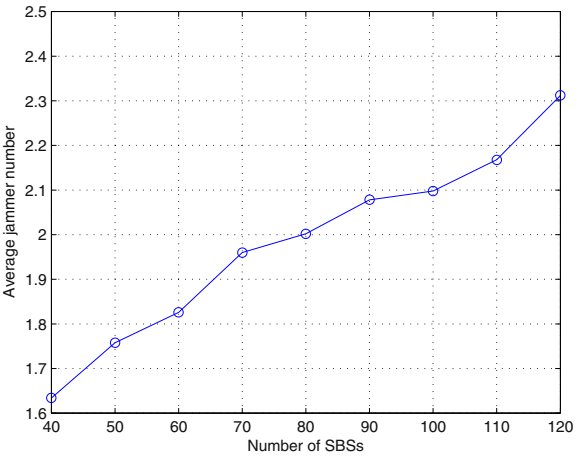

Fig. 10 The average number of jammers each MUE has as a function of different number of SBSs

of the general small-cell layer is enhanced. More specifically, no less than 10 % has been improved, compared with the situation when all players work alone. In addition, a more detailed inspect shows that this improvement is mostly contributed by the jammer SBSs. The jammers share a 61.39∼70.79 % improvement as the SBS number varies from 40 to 120. This is mainly due to the fact that the jammers are granted additional frequency resource so that a notably improvement can be achieved, while the non-jammer SBSs, who stay in a non-cooperative status, obtain almost no benefit. Though not significant, the non-jammer SBSs still share a slight improvement. The reason is that a proportion α of jamming power is transitted to the MUE's channel by the jammers, alleviating the co-layer interference among co-channel SBSs. This simulation result fully demonstrates the win-win property

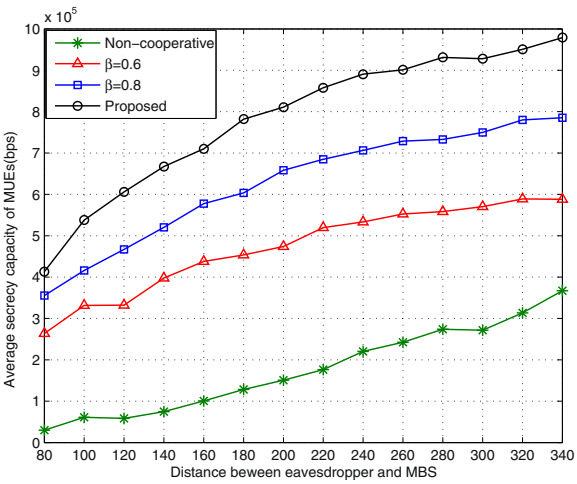

Fig. 11 Secrecy capacity of MUEs as a function of distance between the eavesdropper and MBS

of the cooperation. The players who form a non-singleton coalition actually gain far more revenue than acting alone. Note that the decreasing trend of all curves in Fig. 9 is due to the more severe co-layer interference when the number of SBSs increases.

Figure 10 plots the average number of jammers that each MUE possesses in the final partition versus the SBS number. This gives us an insight on the average coalition size in the system. From what can be seen from Fig. 10, although the average number of jammers grows as the number of SBSs increases, the variation is rather small. The total number of jammers is around 20, no matter how many SBSs are there. The percentage of jammers drops from 40.85 to 19.27 %, when the number of SBSs varies from 40 to 120. This can well interpret the decline of the overall SBSs' curves in Fig. 9. As analyzed previously, the SBSs are classified into to the high rate jammers and the relatively low rate non-jammers. The average capacity of whole SBSs is actually the average result of two kinds of SBSs. With the falling percentage of jammers, the average capacity gain of the small-cell layer consequently has a descending trend.

To study the effect of the eavesdropper's location on the secrecy capacity and the cooperation among the players, we plot the average secrecy capacity of MUE as a function of the distance between the eavesdropper and MBS in Fig. 11. Due to the characteristic of centrosymmetry, we locate the eavesdropper that is d meters away from MBS at $(d, 0)$. In Fig. 11, the average secrecy capacity keeps growing as the eavesdropper moves toward the cell edge. The reason is obvious. A closely spaced eavesdropper has a relatively high quality channel gain between itself and MBS, which gives it an advantage on intercepting the messages of other MUEs. However, the channel gain recedes when the eavesdropper moves further, leading to an improved secrecy performance of the network.

5 Conclusions

In this paper, we consider the secrecy communication in ultra-dense networks and extend the study from a single-user case to multi-user and multi-jammer scenario. In order to protect the MUEs from being overheard by the eavesdropper, we exploit the SBSs in the system to provide jamming for MUEs. The interaction between the MUEs and SBSs has been formulated as a coalition formation game with non-transferable utility in partition form. In addition, we propose an SCSL scheme to effectively encourage the SBSs to cooperate. We study the properties and convergence of the game and propose a novel algorithm to solve it in a distributed manner. The simulation result shows that more than half of the MUEs would be completely intercepted by the eavesdropper in a non-cooperative condition. By adopting the proposed algorithm, almost all the MUEs can obtain a non-zero secrecy capacity and the secrecy capacity of the macro-layer is increased by four times. In addition, the capacity in small-cell layer also gains a 16.92 % improvement on average.

Acknowledgement
This work is supported by National 863 Project (2014AA01A701) and National Nature Science Foundation of China (61372113,61421061).

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

Author details
[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China. [2]Department of Information and Communication Technology, University of Agdar, Kristiansand, Norway.

Received: 11 March 2016 Accepted: 19 August 2016
Published online: 06 September 2016

References

1. Qualcomm Incorporated, The 1000x data challenge (2013). Qualcomm Incorporated. https://www.qualcomm.com/invention/1000x
2. N Saquib, E Hossain, BL Long, IK Dong, Interference management in OFDMA femtocell networks: issues and approaches. IEEE Wirel. Commun. **19**(3), 86–95 (2012)
3. J Xu, J Wang, Y Zhu, Y Yang, X Zheng, S Wang, L Liu, K Horneman, Y Teng, Cooperative distributed optimization for the hyper-dense small cell deployment. IEEE Commun. Mag. **52**(5), 61–67 (2014)
4. K Hosseini, H Dahrouj, R Adve, in *IEEE Global Communications Conference (GLOBECOM)*. Distributed Clustering and Interference Management in Two-Tier Networks (IEEE, California, USA, 2012), pp. 4267–4272
5. M Bennis, SM Perlaza, P Blasco, H Zhu, HV Poor, Self-organization in small cell networks: a reinforcement learning approach. IEEE Trans. Wirel. Commun. **12**(7), 3202–3212 (2013)
6. S Shen, TM Lok, Dynamic power allocation for downlink interference management in a two-tier OFDMA network. IEEE Trans. Veh. Technol. **62**(8), 4120–4125 (2013)
7. A Hatoum, R Langar, N Aitsaadi, R Boutaba, G Pujolle, in *IEEE Global Communications Conference (GLOBECOM)*. QoS-Based Power Control and Resource Allocation in OFDMA Femtocell Networks (IEEE, California, USA, 2012), pp. 5116–5122
8. Z Luo, M Ding, H Luo, Dynamic small cell on/off scheduling using stackelberg game. IEEE Commun. Lett. **18**(9), 1615–1618 (2014)
9. K Son, E Oh, B Krishnamachari, Energy-efficient design of heterogeneous cellular networks from deployment to operation. Comput. Netw. **78**, 95–106 (2015)
10. Y Wang, Y Zhang, Y Chen, R Wei, Energy-efficient design of two-tier femtocell networks. EURASIP J. Wirel. Commun. Netw. **2015**(1), 1–15 (2015)
11. S Hamouda, M Zitoun, S Tabbane, Win–win relationship between macrocell and femtocells for spectrum sharing in LTE-A. IET Commun. **8**(7), 1109–1116 (2014)
12. Y Yang, TQ Quek, Optimal subsidies for shared small cell networks—a social network perspective. IEEE J. Sel. Top. Sig. Process. **8**(4), 690–702 (2014)
13. LC Tseng, FT Chien, D Zhang, RY Chang, WH Chung, C Huang, Network selection in cognitive heterogeneous networks using stochastic learning. IEEE Commun. Lett. **17**(12), 2304–2307 (2013)
14. H-S Jo, YJ Sang, P Xia, JG Andrews, Heterogeneous cellular networks with flexible cell association: A comprehensive downlink SINR analysis. IEEE Trans. Wirel. Commun. **11**(10), 3484–3495 (2012)
15. X Duan, X Wang, Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Commun. Mag. **53**(4), 28–35 (2015)
16. HV Poor, Information and inference in the wireless physical layer. IEEE Wirel. Commun. **19**(1), 40–47 (2012)
17. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)

18. E Tekin, A Yener, The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming. IEEE Trans. Inf. Theory. **54**(6), 2735–2751 (2008)
19. R Zhang, L Song, Z Han, B Jiao, Physical layer security for two-way untrusted relaying with friendly jammers. IEEE Trans. Veh. Technol. **61**(8), 3693–3704 (2012)
20. R Zhang, L Song, Z Han, B Jiao, in *IEEE International Conference on Communications (ICC)*. Distributed Coalition Formation of Relay and Friendly Jammers for Secure Cooperative Networks (IEEE, Kyoto, Japan, 2011), pp. 1–6
21. G Zheng, L-C Choo, K-K Wong, Optimal cooperative jamming to enhance physical layer security using relays. IEEE Trans. Sig. Process. **59**(3), 1317–1322 (2011)
22. I Stanojev, A Yener, Improving secrecy rate via spectrum leasing for friendly jamming. IEEE Trans. Wirel. Commun. **12**(1), 134–145 (2013)
23. N Mokari, S Parsaeefard, H Saeedi, P Azmi, Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users. IEEE Trans. Wirel. Commun. **13**(2), 1058–1073 (2014)
24. Y Wu, K Liu, An information secrecy game in cognitive radio networks. IEEE Trans. Inf. Forensic Secur. **6**(3), 831–842 (2011)
25. Z Han, N Marina, M Debbah, A Hjørungnes, in *IEEE International Conference on Mobile Ad-hoc and Sensor Networks*. Improved Wireless Secrecy Rate Using Distributed Auction Theory (IEEE, China, 2009), pp. 442–447
26. J Yue, B Yang, X Guan, in *IEEE International Conference on Wireless Communications & Signal Processing (WCSP)*. Fairness-Guaranteed Pricing and Power Allocation with a Friendly Jammer Against Eavesdropping (IEEE, Huangshan, China, 2012), pp. 1–6
27. J Qu, Y Cai, J Lu, A Wang, J Zheng, W Yang, N Weng, in *IET International Conference on Cyberspace Technology (CCT)*. Power Allocation Based on Stackelberg Game in a Jammer-Assisted Secure Network (IET, Beijing, China, 2013), pp. 347–352
28. Z Zhang, L Song, Z Han, W Saad, Coalitional games with overlapping coalitions for interference management in small cell networks. IEEE Trans. Wirel. Commun. **13**(5), 2659–2669 (2014)
29. W Saad, Z Han, A Hjørungnes, D Niyato, E Hossain, Coalition formation games for distributed cooperation among roadside units in vehicular networks. IEEE J. Sel. Areas Commun. **29**(1), 48–60 (2011)
30. F Pantisano, M Bennis, W Saad, M Debbah, Spectrum leasing as an incentive towards uplink macrocell and femtocell cooperation. IEEE J. Sel. Areas Commun. **30**(3), 617–630 (2012)
31. W Saad, Z Han, Baş,ar, M Debbah, A Hjørungnes, Hedonic coalition formation for distributed task allocation among wireless agents. IEEE Trans. Mob. Comput. **10**(9), 1327–1344 (2010)
32. A Bogomolnaia, MO Jackson, The stability of hedonic coalition structures. Game Econ. Behav. **38**(2), 201–230 (2002)
33. RM Thrall, WF Lucas, N-person games in partition function form. Nav. Res. Logist. Q. **10**(1), 281–298 (1963)
34. BM Roger, *Game Theory: Analysis of Conflict*. (Cambridge: Harvard University Press, USA, 1991)
35. D Ray, *A Game-theoretic Perspective on Coalition Formation*. (Oxford University Press, New York, USA, 2007)
36. Z Han, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. (Cambridge University Press, Cambridge, UK, 2012)
37. ML Littman, in *Eighteenth International Conference on Machine Learning*. Friend-or-Foe Q-Learning in General-Sum Games, (2001), pp. 322–328