Mobile Netw Appl (2011) 16:231–245
DOI 10.1007/s11036-010-0275-1

Distributed Coalition Formation Games for Secure Wireless Transmission

Walid Saad · Zhu Han · Tamer Başar · Mérouane Debbah · Are Hjørungnes

Published online: 11 November 2010

Abstract Cooperation among wireless nodes has been recently proposed for improving the physical layer (PHY) security of wireless transmission in the presence of multiple eavesdroppers. While existing PHY security literature answered the question "what are the link-level *secrecy rate* gains from cooperation?", this paper attempts to answer the question of "how to achieve those gains in a practical decentralized wireless network and in the presence of a cost for information exchange?". For this purpose, we model the PHY security cooperation problem as a coalitional game with non-transferable utility and propose a distributed algorithm for coalition formation. Using the proposed algorithm, the wireless users can cooperate and self-organize into disjoint independent coalitions, while maximizing their secrecy rate taking into account the costs during information exchange. We analyze the resulting coalitional structures for both decode-and-forward and amplify-and-forward cooperation and study how the users can adapt the network topology to environmental changes such as mobility. Through simulations, we assess the performance of the proposed algorithm and show that, by coalition formation using decode-and-forward, the average secrecy rate per user is increased of up to 25.3 and 24.4% (for a network with 45 users) relative to the non-cooperative and amplify-and-forward cases, respectively.

Keywords physical layer security · coalitional games · game theory · secure communication

This work was done, in part, during the stay of Walid Saad at the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign and was supported by the research council of Norway through the projects 183311/S10, 176773/S10, and 18778/V11 and by NSF grants CNS-0910461, CNS-0905556, CNS-0953377, and ECCS-1028782. A preliminary version of this paper appears in the Proceedings of the 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks [25].

W. Saad (✉) · A. Hjørungnes
UNIK—University Graduate Center,
University of Oslo, Oslo, Norway
e-mail: saad.walid@gmail.com

A. Hjørungnes
e-mail: arehj@unik.no

Z. Han
Electrical and Computer Engineering Department,
University of Houston, Houston, TX, USA
e-mail: zhan2@mail.uh.edu

T. Başar
Coordinated Science Laboratory, University of Illinois
at Urbana Champaign, 1308 West Main,
Urbana, IL 61801, USA
e-mail: basar1@illinois.edu

M. Debbah
SUPELEC, Plateau de Moulon, 3 rue Joliot-Curie Bureau
5-24, 91192, Gif Sur Yvette Cedex, France
e-mail: merouane.debbah@supelec.fr

1 Introduction

With the recent emergence of ad hoc and decentralized networks, researchers have been seeking alternative ways to secure wireless transmission while avoiding the overhead that classical cryptograph may yield. This effort has led to an increased attention on studying the ability of the physical layer (PHY) to provide secure wireless communication. The main idea is to exploit the

wireless channel PHY characteristics such as fading or noise for improving the reliability of wireless transmission. While PHY security is not a substitute for classical cryptography, it does indeed provide an alternative that can complement traditional encryption based security methods and, potentially, ease their implementation in large scale future wireless networks. For instance, one key advantage of PHY security is the possibility of providing, using channel coding and information theoretical techniques, guarantees on security (at the physical layer) irrespective of time or of the computational resources available at the attacker [1–6]. When dealing with PHY security, the reliability of a wireless channel is quantified by the rate of secret information sent from a wireless node to its destination in the presence of eavesdroppers, i.e., the so-called *secrecy rate*. The maximal achievable secrecy rate is referred to as the *secrecy capacity*. The study of this security aspect began with the pioneering work of Wyner over the wire-tap channel [1] and was followed up in [2, 3] for the scalar Gaussian wire-tap channel and the broadcast channel, respectively.

Recently, there has been a growing interest in carrying out these studies unto the wireless and the multi-user channels [4–11]. For instance, in [4] and [5], the authors study the secrecy capacity region for both the Gaussian and the fading broadcast channels and propose optimal power allocation strategies. In [6], the secrecy level in multiple access channels from a link-level perspective is studied. Further, multiple antenna systems have been proposed in [8] for ensuring a non-zero secrecy capacity. The work in [9, 10] presents a performance analysis for using cooperative beamforming (with no cost for cooperation), with decode-and-forward and amplify-and-forward relaying, to improve the secrecy rate of a single cluster consisting of one source node and a number of relays. Moreover, in [11], the use of friendly jammer nodes has been proposed as a technique for reducing the effect of the eavesdroppers and improving the secrecy rates of trusted nodes. Briefly, the majority of the existing literature is devoted to the information theoretic analysis of link-level performance gains of secure communications with no information exchange cost, notably when a source node cooperates with some relays as in [9, 10]. While this literature studied the performance of some cooperative schemes, no work seems to have investigated how a number of users, each with its own data, can interact and cooperate at network-wide level to improve their secrecy rate.

The main contribution of this work is to propose distributed cooperation strategies, making use of coalitional game theory [12], which allow to study the interactions between a network of users that seek to secure their communication in the presence of multiple eavesdroppers. Another major contribution is to study the impact on the network topology and dynamics of the inherent tradeoff that exists between the PHY security cooperation gains in terms of secrecy rate and the information exchange costs. In other words, while the earlier work answered the question of "what are the secrecy rate gains from cooperation?", here, we seek to answer the question of "how to achieve those gains in a practical decentralized wireless network and in the presence of a cost for information exchange?". We model the problem as a non-transferable coalitional game and propose a distributed algorithm for autonomous coalition formation based on well suited concepts from cooperative games. Through the proposed algorithm, each user autonomously decides to form or break a coalition for maximizing its utility in terms of secrecy rate while accounting for the loss of secrecy rate during information exchange. We show that independent disjoint coalitions form in the network, due to the cooperation cost, and we study their properties for both the decode-and-forward and amplify-and-forward cooperation models. Simulation results show that, by coalition formation using decode-and-forward, the average secrecy rate per user is increased by up to 25.3 and 24.4% relative to the non-cooperative and amplify-and-forward cases, respectively. Further, the results show how the users can self-organize and adapt the topology to mobility. Note that, this paper is an extension of the previous conference version in [25].

The rest of this paper is organized as follows: Section 2 presents the system model. Section 3 presents the game formulation and properties. In Section 4 we devise the coalition formation algorithm. Simulation results are presented and analyzed in Section 5. Finally, conclusions are drawn in Section 6.

2 System model

Consider a network having N transmitters (e.g. mobile users) sending data to M receivers (destinations) in the presence of K eavesdroppers that seek to tap into the transmission of the users. Users, receivers and eavesdroppers are unidirectional-single-antenna nodes. We define $\mathcal{N} = \{1, \ldots, N\}$, $\mathcal{M} = \{1, \ldots, M\}$ and $\mathcal{K} = \{1, \ldots, K\}$ as the sets of users, destinations, and eavesdroppers, respectively. We consider only the case of multiple eavesdroppers, hence, we have $K > 1$ although the case of a single eavesdropper can be easily accommodated. Furthermore, let h_{i,m_i} denote the complex baseband channel gain between user $i \in \mathcal{N}$ and its

destination $m_i \in \mathcal{M}$ and $g_{i,k}$ denote the channel gain between user $i \in \mathcal{N}$ and eavesdropper $k \in \mathcal{K}$. We consider a line of sight channel model with $h_{i,m_i} = d_{i,m_i}^{-\frac{\mu}{2}} e^{j\phi_{i,m_i}}$ with d_{i,m_i} the distance between user i and its destination m_i, μ the pathloss exponent, and ϕ_{i,m_i} the phase offset. A similar model is also used for the user-eavesdropper channel.

In this model, we consider that the transmitters in $\mathcal{N}$ are all trusted and they are aware of the presence of malicious nodes, i.e., the eavesdroppers in $\mathcal{K}$. Further, it is considered that the nodes are aware of their channel to their destination and to the eavesdroppers, which is an assumption commonly used in most PHY security related literature [1–10] (and references therein). For the considered channel model, as the nodes are aware of the eavesdroppers' and receivers' locations, they can estimate the channels. We note that the model, algorithm, and analysis of this paper can readily accommodate other channel models, subject to, however, modification of some practical aspects. For example, for rapidly varying channels, the nodes may be required to perform advanced signal processing techniques such as those in [13], in order to acquire estimates of the channels to the eavesdroppers and the destinations.

The proposed model is motivated by various practical applications for physical layer security. For example, the eavesdroppers can be thought of as areas where the trusted transmitters suspect the presence of malicious nodes, and, hence, they seek to make sure that no eavesdropping is done through these locations. Such a model is, for example, applicable in the battlefield where nodes belonging to a certain party attempt to secure certain locations suspected of exhibiting malicious behavior. Another possible scenario is the case where the wireless nodes engage in cooperation only with other nodes that have authenticated with the network, e.g., through a database such as the HLR/VLR of 3G/4G wireless systems, while assuming that all other nodes, i.e., unauthenticated nodes, are malicious eavesdroppers. Hence, the proposed model is suited to several potential scenarios. Further, we note that, our current analysis can also serve to provide an upper bound for future work where the analysis pertaining to the case where the eavesdropper' identity and their locations are not known will be tackled (in that case although the cooperation model needs to be modified and a trust scheme needs to be integrated, the PHY security coalitional game model presented in the following sections can be readily applied).

For multiple access, we consider a TDMA transmission, whereby, in a non-cooperative manner, each user occupies a single time slot. Within a single slot, the amount of reliable information transmitted from the user i occupying the slot to its destination m_i is quantified through the *secrecy rate* C_{i,m_i} defined as follows [4]:

$$C_{i,m_i} = \left(C^d_{i,m_i} - \max_{1 \le k \le K} C^e_{i,k} \right)^+, \tag{1}$$

where C^d_{i,m_i} is the capacity for the transmission between user i and its destination $m_i \in \mathcal{M}$, $C^e_{i,k}$ is the capacity of user i at the eavesdropper $k \in \mathcal{K}$, and $a^+ \triangleq \max(a, 0)$. Note that the secrecy rate in Eq. 1 is shown to be achievable in [14] using Gaussian inputs.

In a non-cooperative approach, due to the broadcast nature of the wireless channel, the transmission of the users can be overheard by the eavesdroppers, which reduces their secrecy rate as clearly expressed in Eq. 1. For improving their performance and increasing their secrecy rate, the users can collaborate by forming coalitions. Within every coalition, the users can utilize collaborative beamforming techniques for improving their secrecy rates. In this context, every user i member of a coalition S can cooperate with its partners in S by dividing its slot into two durations:

1. In the first duration, user i broadcasts its data to the other members of coalition S.
2. In the second duration, coalition S performs collaborative beamforming. Thus, all the members of coalition S relay a weighted version of user i's signal to its destination.

Although finding an optimal cooperation scheme that maximizes the secrecy rate is quite complex [9], one approach for cooperation is to null the signal at the eavesdroppers, i.e., impose $C^e_{i,k} = 0, \forall k \in \mathcal{K}$, hence, improving their secrecy rate as compared to the non-cooperative rate in Eq. 1 [9]. Each coalition $S \subseteq \mathcal{N}$ that forms in the network is able to transmit within all the time slots previously held by its users. Thus, in the presence of cooperating coalitions, the TDMA system schedules one coalition per time slot. During a given slot, the coalition acts as a single entity for transmitting the data of the user that owns the slot. Figure 1 shows an illustration of this model for $N = 9$ users, $M = 2$ destinations, and $K = 2$ eavesdroppers.

Furthermore, we define a fixed transmit power *per time slot* $\tilde{P}$ which constrains *all the users* that are transmitting within a given slot. In a non-cooperative manner, this power constraint applies to the single user occupying the slot, while in the cooperative case this *same* power constraint applies to the entire coalition occupying the slot. Such an assumption is quite common [15–17], whereby a power constraint per slot is considered to apply to the total power of *all*

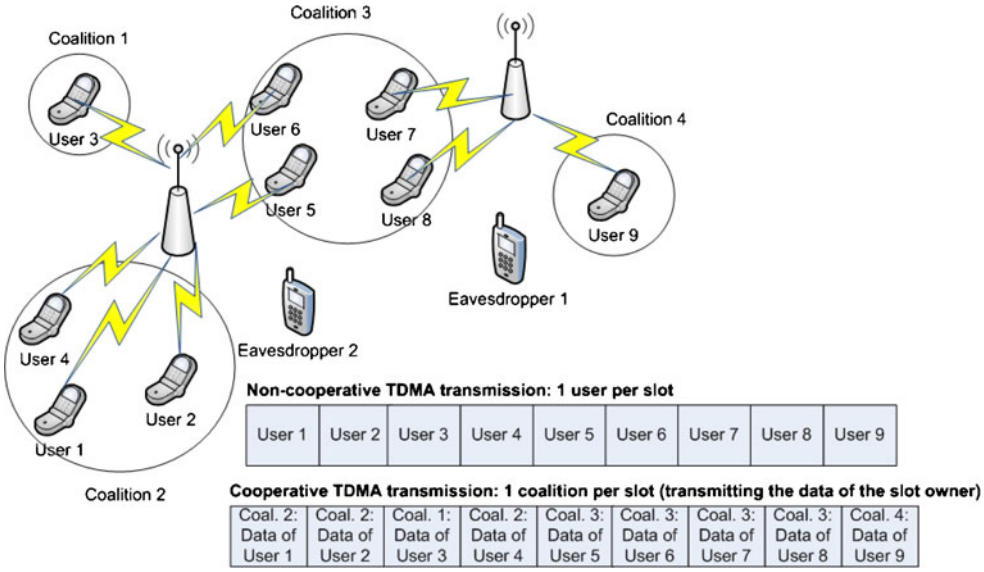

Fig. 1 System model for physical layer security coalitional game

transmitters in this slot. The main rationale for such a condition is that, on the average, due to varying users' locations (or channels), the users will experience fluctuations of their transmit power which will be compensated by other users in the same coalition so as to meet fixed constraint per slot. For every coalition S, during the time slot owned by user $i \in S$, user i utilizes a portion of the available power $\tilde{P}$ for information exchange (first stage) while the remaining portion P_i^S is used by the coalition S to transmit the actual data to the destination m_i of user i (second stage). For information exchange, user $i \in S$ can broadcast its information to the farthest user $\hat{i} \in S$, by doing so all the other members of S can also obtain the information due to the broadcast nature of the wireless channel. This information exchange incurs a power cost $\bar{P}_{i,\hat{i}}$ given by

$$\bar{P}_{i,\hat{i}} = \frac{\nu_0 \cdot \sigma^2}{|q_{i,\hat{i}}|^2}, \tag{2}$$

where ν_0 is a target average signal-to-noise ratio (SNR) for information exchange, σ^2 is the noise variance and $q_{i,\hat{i}}$ is the channel gain between users i and $\hat{i}$. The remaining power that coalition S utilizes for the transmission of the data of user i during the remaining time of this user's slot is

$$P_i^S = \left(\tilde{P} - \bar{P}_{i,\hat{i}}\right)^+. \tag{3}$$

For every coalition S, during the transmission of the data of user i to its destination, the coalition members can cooperate, using either decode-and-forward (DF) or amplify-and-forward (AF), and, hence, weight their signals in a way to *completely null* the signal at the eavesdroppers. In DF, the basic idea is that, once the coalition members that are acting as relays decode the noisy signal that was received in the information exchange phase from the source, they re-encode this signal before performing beamforming, i.e., transmitting a weighted version of the re-encoded signal. In contrast, for AF, in the first phase, the coalition members that are acting as relays do not decode the noisy signal, instead, they perform beamforming by weighting the noisy version of the signal received during the information exchange phase and transmitting it. Hence, while in DF the relays decode the signal and re-encode it and, then, transmit a weighted signal of the re-encoded version, in AF, the relays weight the entire received signal, i.e., including the noise, and then transmit this weighted version. Thus, although DF can provide a better performance, AF is less complex due to the unnecessary need for decoding and re-encoding the signal. We refer to [9, 10, 18, 19] and references therein for a detailed and exhaustive description of applications and additional aspects of DF and AF relaying, which are out of the scope of this paper. Further, for any coalition S the signal weights and the "user-destination" channels are represented by the $|S| \times 1$ vectors $\boldsymbol{w}_S = [w_{i_1}, \ldots, w_{i_{|S|}}]^H$ and $\boldsymbol{h}_S = [h_{i_1,m_1}, \ldots, h_{i_{|S|},m_{|S|}}]^H$, respectively.

By nulling the signals at the eavesdropper through DF cooperation within coalition S, the secrecy rate achieved by user $i \in S$ at its destination m_i during user i's time slot becomes [9, Eq. 14]

$$C_{i,m_i}^{S,\mathrm{DF}} = \frac{1}{2}\log_2\left(1 + \frac{\left(\boldsymbol{w}_S^{*,\mathrm{DF}}\right)^H \boldsymbol{R}_S \boldsymbol{w}_S^{*,DF}}{\sigma^2}\right), \tag{4}$$

where $\boldsymbol{R}_S = \boldsymbol{h}_S \boldsymbol{h}_S^H$, σ^2 is the noise variance, and $\boldsymbol{w}_S^{*,\mathrm{DF}}$ is the weight vector that maximizes the secrecy rate

while nulling the signal at the eavesdropper with DF cooperation and can be found using [9, Eq. 20]. In Eq. 4, the factor $\frac{1}{2}$ accounts for the fact that half of the slot of user i is reserved for information exchange.

For AF, we define, during the transmission slot of a user $i \in S$ member of a coalition S, the $|S| \times 1$ vector $\boldsymbol{a}_S^i$ with every element $a_{S,j}^i = \sqrt{\bar{P}_{i,\hat{i}}} q_{i,j} h_{j,m_j}$, $\forall j \neq i$ ($q_{i,j}$ is the channel between users i and j and $\bar{P}_{i,\hat{i}}$ is the power used by user i for information exchange as per Eq. 2) and $a_{S,i}^i = \sqrt{\bar{P}_{i,\hat{i}}} h_{i,m_i}$ and the $|S| \times |S|$ diagonal matrix $\boldsymbol{U}_S^i$ with every diagonal element $u_{S,j,j}^i = |h_{j,m_j}|^2$ $\forall j \neq i$ and $u_{S,i,i}^i = 0$. Given these definitions and by nulling the signals at the eavesdropper through AF cooperation within coalition S, the secrecy rate achieved by user $i \in S$ at its destination m_i during user i's time slot becomes [10, Eq. 3]

$$C_{i,m_i}^{S,\mathrm{AF}} = \frac{1}{2} \log_2 \left(1 + \frac{(\boldsymbol{w}_S^{*,\mathrm{AF}})^H \boldsymbol{R}_a \boldsymbol{w}_S^{*,\mathrm{AF}}}{(\boldsymbol{w}_S^{*,\mathrm{AF}})^H \boldsymbol{U}_S^i \boldsymbol{w}_S^{*,\mathrm{AF}} + 1)\sigma^2} \right), \quad (5)$$

where $\boldsymbol{R}_a = \boldsymbol{a}_S^i (\boldsymbol{a}_S^i)^H$, and $\boldsymbol{w}_S^{*,\mathrm{AF}}$ is the weight vector that maximizes the secrecy rate while nulling the signal at the eavesdropper with AF cooperation and can be found using [10, Eqs. 14, 15]. Note that for AF, as seen in Eq. 5, there is a stronger dependence on the channels (through the matrix $\boldsymbol{R}_a$) between the cooperating users in both the first and second phase of cooperation, unlike in DF, where this dependence is solely through the power in Eq. 2 during the information exchange phase. Further, for AF, as the cooperating users amplify a noisy version of the signal, the noise is also amplified, which can reduce the cooperation gains, as seen through the term $(\boldsymbol{w}_S^{*,\mathrm{AF}})^H \boldsymbol{U}_S^i \boldsymbol{w}_S^{*,\mathrm{AF}}$.

Further, it must be stressed that, although the models for AF and DF cooperation in Eqs. 4 and 5 are inspired from [9, 10], our work and contribution differ significantly from [9, 10]. While the work in [9, 10] is solely dedicated to finding the optimal weights in Eqs. 4 and 5, and presenting a link-level performance analysis for a single cluster of neighboring nodes with no cost for cooperation, our work seeks to perform a network-level analysis by modeling the interactions among a network of users that seek to cooperate, in order to improve their performance, using either the DF or AF protocols in the presence of costs for information exchange. Hence, the main focus of this paper is modeling the user's behavior, studying the network dynamics and topology, and analyzing the network-level aspects of cooperation in PHY security problems. In this regard, the remainder of this paper is devoted to an investigation of how a network of users can cooperate, through the protocols described in this section, and improve the security of their wireless transmission, i.e., their secrecy rate.

Finally, note that, although the proposed model considered TDMA transmission for multiple access, the algorithm and coalitional game formulation can be extended to accommodate other schemes as well, such as FDMA or CSMA. Nonetheless, when considering alternative multiple access schemes, one must modify accordingly the benefits and costs from cooperation, in order to capture the properties of the considered multiple access protocol.

3 Physical layer security as a coalitional game

The proposed PHY security problem can be modeled as an $(\mathcal{N}, V)$ coalitional game with a non-transferable utility [12, 20] where V is a mapping such that for every coalition $S \subseteq \mathcal{N}$, $V(S)$ is a closed convex subset of $\mathbb{R}^{|S|}$ that contains the payoff vectors that players in S can achieve. Thus, given a coalition S and denoting by $\phi_i(S)$ the payoff of user $i \in S$ during its time slot, we define the coalitional value set, i.e., the mapping V, as follows

$$V(S) = \{\boldsymbol{\phi}(S) \in \mathbb{R}^{|S|} |\ \forall i \in S\ \phi_i(S) = (v_i(S) - c_i(S))^+ \text{ if } P_i^S > 0, \text{ and } \phi_i(S) = -\infty \text{ otherwise.}\}, \quad (6)$$

where $v_i(S) = C_{i,m_i}^S$ is the gain in terms of secrecy rate for user $i \in S$ given by Eq. 4 while taking into account the available power P_i^S in Eq. 3 and $c_i(S)$ is a cost function that captures the loss for user $i \in S$, in terms of secrecy rate, that occurs during information exchange. Note that, when *all* the power is spent for information exchange, the payoff $\phi_i(S)$ of user i is set to $-\infty$ since, in this case, the user has clearly no interest in cooperating.

With regard to the secrecy cost function $c_i(S)$, when a user $i \in S$ sends its information to the farthest user $\hat{i} \in S$ using a power level $\bar{P}_{i,\hat{i}}$, the eavesdroppers can overhear the transmission. This security loss is quantified by the rate at the eavesdroppers resulting from the information exchange and which, for a particular eavedropper $k \in \mathcal{K}$, is given by $\hat{C}_{i,k}^e = \frac{1}{2} \log (1 + \frac{\bar{P}_{i,\hat{i}} |g_{i,k}|^2}{\sigma^2})$ and the cost function $c(S)$ can be defined as

$$c_i(S) = \max (\hat{C}_{i,1}^e, \ldots, \hat{C}_{i,K}^e). \quad (7)$$

In general, coalitional game based problems seek to characterize the properties and stability of the grand coalition of all players since it is generally assumed that the grand coalition maximizes the utilities of the players [20]. In our case, although cooperation improves the secrecy rate as per Eq. 6 for the users in the TDMA

network; the utility in Eq. 6 also accounts for two types of cooperation costs:(i)- The fraction of power spent for information exchange as per Eq. 3 and, (ii) the secrecy loss during information exchange as per Eq. 7 which can strongly limit the cooperation gains. Therefore, for the proposed $(\mathcal{N}, v)$ coalitional game we have:

Property 1 *For the proposed* $(\mathcal{N}, V)$ *coalitional game, the grand coalition of all the users* seldom *forms due to the various costs for information exchange. Instead, disjoint independent coalitions will form in the network.*

Proof Given a number of users positioned at different locations within the wireless network, cooperation for improving the secrecy rate entails costs, as previously mentioned, in terms of secrecy loss and power loss during information exchange as per Eqs. 2 and 7. Hence, in a practical wireless network where the users are located at different positions, it is highly likely that, when they attempt to cooperate for forming the grand coalition $\mathcal{N}$ of all users, either: (i)- there exists a pair of users $i, j \in \mathcal{N}$ that are distant enough to require an information power cost of $\tilde{P}$, and hence they have no incentive to join the grand coalition, or (ii)- there exists a user $i \in \mathcal{N}$ with payoff in the grand coalition $\phi_i(\mathcal{N}) = 0$ due to the secrecy loss as captured by Eq. 7, hence this user i has incentive to deviate from the grand coalition. Clearly, by accounting for the various cooperation costs, the grand coalition of all users will *seldom* form (it only forms if all users are very close, which is unrealistic in a large scale wireless network) and hence, the network structure consists of disjoint independent coalitions. □

Due to this property, traditional solution concepts for coalitional games, such as the core [20], may not be applicable [12]. In fact, in order for the core to exist, as a solution concept, a coalitional game must ensure that the grand coalition, i.e., the coalition of all players will form. However, as seen in Fig. 1 and corroborated by Property 1, in general, due to the cost for coalition formation, the grand coalition will not form. Instead, independent and disjoint coalitions appear in the network as a result of the collaborative beamforming process. In this regard, the proposed game is classified as a *coalition formation game* [12], and the objective is to find the coalitional structure that will form in the network, instead of finding only a solution concept, such as the core, which aims mainly at stabilizing the grand coalition.

Furthermore, for the proposed $(\mathcal{N}, V)$ coalition formation game, a constraint on the coalition size, imposed by the nature of the cooperation protocol exists as follows:

Remark 1 For the proposed $(\mathcal{N}, V)$ coalition formation game, the size of any coalition $S \subseteq \mathcal{N}$ that will form in the network must satisfy $|S| > K$ for both DF and AF cooperation.

This is a direct result of the fact that, for nulling K eavesdroppers, at least $K + 1$ users must cooperate, otherwise, no weight vector can be found to maximize the secrecy rate while nulling the signal at the eavesdroppers.

4 Distributed Coalition formation algorithm

4.1 Coalition formation algorithm

Coalition formation has recently attracted increased attention in game theory [12, 21, 22]. The goal of coalition formation games is to find algorithms for characterizing the coalitional structures that form in a network where the grand coalition is not optimal. For constructing a coalition formation process suitable to the proposed $(\mathcal{N}, V)$ PHY security cooperative game, we require the following definitions [12, 22]:

Definition 1 A *collection* of coalitions, denoted by $\mathcal{S}$, is defined as the set $\mathcal{S} = \{S_1, \ldots, S_l\}$ of mutually disjoint coalitions $S_i \subset \mathcal{N}$. In other words, a collection is any arbitrary group of disjoint coalitions S_i of $\mathcal{N}$ not necessarily spanning all players of $\mathcal{N}$. If the collection spans *all* the players of $\mathcal{N}$; that is $\bigcup_{j=1}^{l} S_j = \mathcal{N}$, the collection is a *partition* of $\mathcal{N}$.

Definition 2 A preference operator or *comparison relation* $\rhd$ is an order defined for comparing two collections $\mathcal{R} = \{R_1, \ldots, R_l\}$ and $\mathcal{S} = \{S_1, \ldots, S_p\}$ that are partitions of the same subset $\mathcal{A} \subseteq \mathcal{N}$ (i.e. same players in $\mathcal{R}$ and $\mathcal{S}$). Therefore, $\mathcal{R} \rhd \mathcal{S}$ implies that the way $\mathcal{R}$ partitions $\mathcal{A}$ is preferred to the way $\mathcal{S}$ partitions $\mathcal{A}$.

For the proposed PHY security coalition formation game, an individual value order, i.e. an order which compares the individual payoffs of the users, is needed due to the non-transferable utility of the game. For this purpose, for the proposed game, we utilize the following order for defining the preferences of the users:

Definition 3 Consider two collections $\mathcal{R} = \{R_1, \ldots, R_l\}$ and $\mathcal{S} = \{S_1, \ldots, S_m\}$ that are partitions

Algorithm 1 One round of the proposed PHY security coalition formation algorithm

Initial State

The network is partitioned by $\mathcal{T} = \{T_1, \ldots, T_k\}$ (At the beginning of all time $\mathcal{T} = \mathcal{N} = \{1, \ldots, N\}$ with non-cooperative users).

Phase 1 - Neighbor Discovery:

a) Each coalition surveys its neighborhood for candidate partners using techniques from [23, 24].

b) For every coalition T_i, the candidate partners lie in the area represented by the intersection of $|T_i|$ circles with centers $j \in T_i$ and radii determined by the distance where the power for information exchange does not exceed $\tilde{P}$ for any user (computed by Eq. 2).

Phase 2 - Adaptive Coalition Formation:

In this phase, coalition formation using merge-and-split occurs.

repeat

A) $\mathcal{F}$ **= Merge(**$\mathcal{T}$**)**; coalitions in $\mathcal{T}$ decide to merge as follows (more details of the merge are in Section 4.1):

a) Each coalition $T_i \in \mathcal{T}$ elects a coalition head $k \in T_i$ to perform negotiations with the neighbors for merge.

b) Sequentially, for each coalition $T_i \in \mathcal{T}$ that is attempting to merge:

b.1) Coalition head $k \in T_i$ exchanges, over a control channel with the neighbors, the details of their members, e.g., channel estimates, capabilities, and locations.

b.2) Coalition head $k \in T_i$, $\forall T_i \in \mathcal{T}$ uses the gathered information to find a group of coalitions to merge with. For doing so, the coalition head enumerates, sequentially, the possible coalitions, of size greater than K (see Remark 1), that it can form with the neighbors that were discovered in Phase 1. This enumeration stops when the head finds a suited coalition to merge with.

b.3) Coalition head $k \in T_i$ signals an intent to cooperate to the coalitions with whom it is interested to merge and which verify the Pareto order.

b.4) Coalition head k will receive an approval to merge, and, subsequently, the merge operation is jointly performed by all concerned coalitions.

B) $\mathcal{T}$ **= Split(**$\mathcal{F}$**)**; coalitions in $\mathcal{F}$ decide to split based on the Pareto order as follows:

a) The members of each coalition coordinate *internally* and attempt to assess whether any split form can be found to satisfy the Pareto order.

b) As the members are part of the same coalition, assessing the payoffs yielded by a split form is easily performed since the members are aware of the identities and characteristics of their partners.

until Merge-and-split terminates.

Phase 3 - Secure Transmission:

Each coalition's users exchange their information and transmit their data within their allotted slots using DF or AF techniques in [9, 10, 18, 19].

The above three phases are repeated periodically during the network operation, allowing a topology that is adaptive to environmental changes such as mobility.

of the same subset $\mathcal{A} \subseteq \mathcal{N}$ (same players in $\mathcal{R}$ and $\mathcal{S}$). For a collection $\mathcal{R} = \{R_1, \ldots, R_l\}$, let the utility of a player j in a coalition $R_j \in \mathcal{R}$ be denoted by $\Phi_j(\mathcal{R}) = \phi_j(R_j) \in V(R_j)$. $\mathcal{R}$ is preferred over $\mathcal{S}$ by *Pareto order*, written as $\mathcal{R} \rhd \mathcal{S}$, iff

$$\mathcal{R} \rhd \mathcal{S} \Longleftrightarrow \{\Phi_j(\mathcal{R}) \geq \Phi_j(\mathcal{S}) \; \forall \; j \in \mathcal{R}, \mathcal{S}\},$$

with *at least one strict inequality* $(>)$ for a player k.

In other words, a collection is preferred by the players over another collection, if at least one player is able to improve its payoff without hurting the other players. Subsequently, for performing autonomous coalition formation between the users in the proposed PHY security game, we construct a distributed algorithm based on two simple rules denoted as "merge" and "split" [12, 22] defined as follows:

Definition 4 Merge Rule - Merge any set of coalitions $\{S_1, \ldots, S_l\}$ whenever the merged form is preferred by the players, i.e., where $\{\bigcup_{j=1}^{l} S_j\} \rhd \{S_1, \ldots, S_l\}$, therefore, $\{S_1, \ldots, S_l\} \rightarrow \{\bigcup_{j=1}^{l} S_j\}$.

Definition 5 Split Rule - Split any coalition $\bigcup_{j=1}^{l} S_j$ whenever a split form is preferred by the players, i.e., where $\{S_1, \ldots, S_l\} \rhd \{\bigcup_{j=1}^{l} S_j\}$, thus, $\{\bigcup_{j=1}^{l} S_j\} \rightarrow \{S_1, \ldots, S_l\}$.

Using the above rules, multiple coalitions can merge into a larger coalition if merging yields a preferred collection based on the Pareto order. This implies that a group of users can agree to form a larger coalition, if at least one of the users improves its payoff without decreasing the utilities of any of the other users. Similarly, an existing coalition can decide to split into smaller coalitions if splitting yields a preferred collection by Pareto order. The rationale behind these rules is that, once the users agree to sign a merge agreement, this agreement can only be broken if all the users approve. This is a family of coalition formation games known as "coalition formation games with partially reversible agreements" [21]. Using the rules of merge and split is highly suitable for the proposed PHY security game due to many reasons. For instance, each merge or split decision can be taken in a distributed manner by each individual user or by each already formed coalition. Further, it is shown in [22] that any arbitrary iteration of merge and split rules terminates, hence, these rules can be used as building blocks in a coalition formation process for the PHY security game.

Accordingly, for the proposed PHY security game, we construct a coalition formation algorithm based on merge-and-split. Each run of the proposed algorithm

consists of three phases: Neighbor discovery, adaptive coalition formation, and transmission, and is summarized in Algorithm 1. In the neighbor discovery phase (Phase 1), each coalition (or user) surveys its environment in order to find possible cooperation candidates. For a coalition S_k the area that is surveyed for discovery is the intersection of $|S_k|$ circles, centered at the coalition members with each circle's radius given by the maximum distance $\bar{r}_i$ (for the circle centered at $i \in S_k$) within which the power cost for user i as given by Eq. 2 does not exceed the total available power $\tilde{P}$. This area is determined by the fact that, if a number of coalitions $\{S_1, \ldots, S_m\}$ attempt to merge into a new coalition $G = \cup_{i=1}^{m} S_i$ which contains a member $i \in G$ such that the power for information exchange needed by i exceeds $\tilde{P}$, then the payoff of i goes to $-\infty$ as per Eq. 6 and the Pareto order can never be verified. Clearly, as the number of users in a coalition increases, the number of circles increases, reducing the area where possible cooperation partners can be found. This implies that, as the size of a coalition grows, the possibility of adding new users decreases, and, hence, the complexity of performing merge also decreases.

Following Phase 1, the adaptive coalition formation phase (Phase 2) begins, whereby the users interact for assessing whether to form new coalitions with their neighbors or whether to break their current coalition. For this purpose, an iteration of sequential merge-and-split rules occurs in the network, whereby each coalition decides to merge (or split) depending on the utility improvement that merging (or splitting) yields. Starting from an initial network partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ of $\mathcal{N}$, the first step in the merge process is that, for every coalition $T_i \in \mathcal{T}$ a coalition head is selected in order to handle the merge part of coalition formation. Over time, the head of a coalition can change in a round robin fashion for example. Subsequently, any random coalition (individual user) can start with the merge process. The coalition head k of a coalition $T_i \in \mathcal{T}$ which debuts the merge process starts by gathering, over a control channel, some information on the characteristics of neighboring coalitions, e.g., channel estimates, locations, and capabilities. Subsequently, using the gathered information, the coalition head begins enumerating, sequentially, the possible coalitions, of size greater than K (Remark 1), that it can form with the neighbors that were discovered in Phase 1. On one hand, if a new coalition $\tilde{T}_i$ which is preferred by the users through Pareto order is identified, this coalition will form by a merge agreement of all its members as described in Algorithm 1. Hence, the merge ends by a final merged coalition T_i^{final} composed of T_i and one or several of coalitions in its vicinity. On the other hand, if T_i is unable to merge with any of the discovered partners, it ends its search and $T_i^{\text{final}} = T_i$.

The algorithm is repeated for the remaining $T_i \in \mathcal{T}$ until all the coalitions have made their merge decisions, resulting in a final partition $\mathcal{F}$. Following the merge process, the coalitions in the resulting partition $\mathcal{F}$ are next subject to split operations, if any is possible. Since the split operation involves members of the *same* coalition, the coalition members can easily coordinate and attempt to assess whether any split form can be found to satisfy the Pareto order. Note that, in the proposed PHY security problem, the coalitions are only interested in splitting into structures that include either singleton users or coalitions of size larger than K or both (Remark 1). Unlike the merge, the split is a local decision to each coalition. An iteration consisting of multiple successive merge-and-split operations is repeated until it terminates. The termination of an iteration of merge and split rules is guaranteed as shown in [22]. It must be stressed that the merge or split decisions can be taken in a distributed way by the users/coalitions without relying on any centralized entity.

In the final transmission phase (Phase 3), the coalitions exchange their information and begin their secure transmission towards their corresponding destinations, in a TDMA manner, one coalition per slot. Every slot is owned by a user who transmits its data with the help of its coalition partners, if that user belongs to a coalition. Hence, in this phase, the user performs the actual beamforming, while transmitting the data of every user within its corresponding slot. For performing beamforming using DF or AF, any of the practical algorithms in [18, 19] can be adopted. As time evolves and the users, eavesdroppers and destinations move (or new users or eavesdroppers enter/leave the network), the users can autonomously self-organize and adapt the network's topology through appropriate merge-and-split decisions during Phase 2. This adaptation to environmental changes is ensured by enabling the users to run the adaptive coalition formation phase periodically in the network.

The proposed Algorithm 1 can be implemented in a distributed manner. As the user can detect the strength of other users' uplink signals (through techniques similar to those used in the ad hoc routing discovery) [23, 24], nearby coalitions can be discovered in Phase 1 for potential cooperation. In fact, during Phase 1, each coalition in the network can easily work out the area within which candidates for merge can be found, as previously explained in this section. Once the neighbors are discovered, the coalitions can perform merge operations based on the Pareto order and using the procedure described in Algorithm 1. The complexity of

the merge operation can grow exponentially with the number of candidates with whom a user i is able to merge (the number of coalitions in the neighboring area which is in general significantly smaller than N). As more coalitions form, the area within which candidates are found is smaller, and, hence, the merge complexity reduces. In addition, whenever a coalition (through its coalition head) finds a candidate to merge with, it automatically goes through with the merge operation, hence, avoiding the need for finding all possible merge forms and reducing further the complexity. Further, each formed coalition can also internally decide to split if its members find a split form by Pareto order. As previously discussed, by using a control channel and the presence of coalition heads, the distributed users can coordinate and then cooperate using our model.

4.2 Partition stability

The result of the proposed Algorithm 1 is a network partition composed of disjoint independent coalitions. The stability of this network partition can be investigated using the concept of a defection function [22].

Definition 6 A *defection* function $\mathbb{D}$ is a function which associates with each partition $\mathcal{T}$ of $\mathcal{N}$ a group of collections in $\mathcal{N}$. A partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ of $\mathcal{N}$ is $\mathbb{D}$-*stable* if no group of players is interested in leaving $\mathcal{T}$ when the players who leave can only form the collections allowed by $\mathbb{D}$.

We are interested in two defection functions [12, 22]. First, the $\mathbb{D}_{hp}$ function which associates with each partition $\mathcal{T}$ of $\mathcal{N}$ the group of all partitions of $\mathcal{N}$ that can form through merge or split and the $\mathbb{D}_c$ function which associates with each partition $\mathcal{T}$ of $\mathcal{N}$ the group of all collections in $\mathcal{N}$. This function allows any group of players to leave the partition $\mathcal{T}$ of $\mathcal{N}$ through *any* operation and create an arbitrary *collection* in $\mathcal{N}$. Two forms of stability stem from these definitions: $\mathbb{D}_{hp}$ stability and a stronger $\mathbb{D}_c$ stability. A partition $\mathcal{T}$ is $\mathbb{D}_{hp}$-stable, if no player in $\mathcal{T}$ is interested in leaving $\mathcal{T}$ through merge-and-split to form other partitions in $\mathcal{N}$; while a partition $\mathcal{T}$ is $\mathbb{D}_c$-stable, if no player in $\mathcal{T}$ is interested in leaving $\mathcal{T}$ through *any* operation (not necessarily merge or split) to form other collections in $\mathcal{N}$.

Hence, a partition is $\mathbb{D}_{hp}$-stable if no coalition has an incentive to split or merge. For instance, a partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ is $\mathbb{D}_{hp}$-stable, if the following two necessary and sufficient conditions are met [12, 22] ($\not\rhd$ is the non-preference operator, opposite of $\rhd$): (i)- For each $i \in \{1, \ldots, m\}$ and for each partition $\{R_1, \ldots, R_m\}$ of $T_i \in \mathcal{T}$ we have $\{R_1, \ldots, R_m\} \not\rhd T_i$, and (ii)- For each $S \subseteq \{1, \ldots, l\}$ we have $\bigcup_{i \in S} T_i \not\rhd \{T_i | i \in S\}$. Using this definition of $\mathbb{D}_{hp}$ stability, we have

Theorem 1 *Every partition resulting from our proposed coalition formation algorithm is $\mathbb{D}_{hp}$-stable.*

Proof Consider a partition $\mathcal{T}$ resulting from the convergence of an iteration of merge-and-split operations such as in Algorithm 1; then no coalition in $\mathcal{T}$ can leave this partition through merge or split. For instance, assume $\mathcal{T} = \{T_1, \ldots, T_l\}$ is the partition resulting from the proposed merge-and-split algorithm. If for any $i \in \{1, \ldots, l\}$ and for any partition $\{S_1, \ldots, S_m\}$ of T_i we assume that $\{S_1, \ldots, S_m\} \rhd T_i$ then the partition $\mathcal{T}$ can still be modified through the application of the split rule on T_i contradicting with the fact that $\mathcal{T}$ resulted from a termination of the merge-and-split iteration; therefore $\{S_1, \ldots, S_m\} \not\rhd T_i$ (first $\mathbb{D}_{hp}$ stability condition verified). A similar reasoning is applicable in order to prove that $\mathcal{T}$ verifies the second condition; since otherwise a merge rule would still be applicable. □

Furthermore, a $\mathbb{D}_c$-stable partition $\mathcal{T}$ is characterized by being a strongly stable partition, which satisfies the following properties: (i)- A $\mathbb{D}_c$-stable partition is $\mathbb{D}_{hp}$-stable, (ii)- A $\mathbb{D}_c$-stable partition is a *unique* outcome of any iteration of merge-and-split and, (iii)- A $\mathbb{D}_c$-stable partition $\mathcal{T}$ is a unique $\rhd$-maximal partition, that is for all partitions $\mathcal{T}' \neq \mathcal{T}$ of $\mathcal{N}$, $\mathcal{T} \rhd \mathcal{T}'$. In the case where $\rhd$ represents the Pareto order, this implies that the $\mathbb{D}_c$-stable partition $\mathcal{T}$ is the partition that presents a *Pareto optimal* utility distribution for all the players.

Clearly, it is desirable that the network self-organizes unto a $\mathbb{D}_c$-stable partition. However, the existence of a $\mathbb{D}_c$-stable partition is not always guaranteed [22]. The $\mathbb{D}_c$-stable partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ of the whole space $\mathcal{N}$ exists if a partition of $\mathcal{N}$ that verifies the following two necessary and sufficient conditions exists [22]:

1. For each $i \in \{1, \ldots, l\}$ and each pair of disjoint *coalitions* S_1 and S_2 such that $\{S_1 \cup S_2\} \subseteq T_i$ we have $\{S_1 \cup S_2\} \rhd \{S_1, S_2\}$.
2. For the partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ a coalition $G \subset \mathcal{N}$ formed of players belonging to different $T_i \in \mathcal{T}$ is $\mathcal{T}$-incompatible if for no $i \in \{1, \ldots, l\}$ we have $G \subset T_i$.

In summary, $\mathbb{D}_c$-stability requires that for all $\mathcal{T}$-incompatible coalitions $\{G\}[\mathcal{T}] \rhd \{G\}$ where $\{G\}[\mathcal{T}] = \{G \cap T_i \; \forall \, i \in \{1, \ldots, l\}\}$ is the projection of coalition G on $\mathcal{T}$. If no partition of $\mathcal{N}$ can satisfy these conditions, then no $\mathbb{D}_c$-stable partition of $\mathcal{N}$ exists. Nevertheless, we have

Lemma 1 *For the proposed* $(\mathcal{N}, v)$ *PHY security coalitional game, the proposed Algorithm 1 converges to the optimal* $\mathbb{D}_c$*-stable partition, if such a partition exists. Otherwise, the final network partition is* $\mathbb{D}_{hp}$*-stable.*

Proof The proof is a consequence of Theorem 1 and the fact that the $\mathbb{D}_c$-stable partition is a unique outcome of any merge-and-split iteration [22] which is the case with any partition resulting from our algorithm. □

Moreover, for the proposed game, the existence of the $\mathbb{D}_c$-stable partition cannot be always guaranteed. For instance, for verifying the first condition for existence of the $\mathbb{D}_c$-stable partition, the users that are members of each of the coalitions must verify the Pareto order through their utility given by Eq. 6. Similarly, for verifying the second condition of $\mathbb{D}_c$ stability, users belonging to all $\mathcal{T}$-incompatible coalitions in the network must verify the Pareto order. Consequently, the existence of such a $\mathbb{D}_c$-stable partition is strongly dependent on the location of the users and eavesdroppers through the individual utilities (secrecy rates). Hence, the existence of the $\mathbb{D}_c$-stable partition is closely tied to the location of the users and the eavesdroppers, which, in a practical ad hoc wireless network are generally random. However, the proposed algorithm will always guarantee convergence to this optimal $\mathbb{D}_c$-stable partition when it exists as stated in Lemma 1. Whenever a $\mathbb{D}_c$-stable partition does not exist, the coalition structure resulting from the proposed algorithm will be $\mathbb{D}_{hp}$-stable (no coalition or individual user is able to merge or split any further).

5 Simulation results and analysis

For simulations, using MATLAB, a square network of 2.5 × 2.5 km is set up with the users, eavesdroppers, and destinations randomly deployed within this area.[1] The destinations are passive data sinks that serve as receivers for the users, i.e., the transmitters. In this network, unless stated otherwise, the users are assigned to the closest destination. Note that, without any loss of generality, other user-destination assignments can also be used. For all simulations, the number of destinations is taken as $M = 2$. Further, the power constraint per slot is set to $\tilde{P} = 10$ mW, the noise level is -90 dBm, and the SNR for information exchange is $v_0 = 10$ dB which implies a neighbor discovery circle radius of 1 km per user. For the channel model, the propagation loss is set to $\mu = 3$. All statistical results are averaged over the random positions of the users, eavesdroppers, and destinations.

In Fig. 2, we show a snapshot of the network structure resulting from the proposed coalition formation algorithm for a randomly deployed network with $N = 15$ users and $K = 2$ eavesdroppers for both DF (dashed lines) and AF (solid lines) protocols. For DF, the users self-organized into 6 coalitions with the size of each coalition strictly larger than K or equal to 1. For example, Users 4 and 15, having no suitable partners for forming a coalition of size larger than 2, do not cooperate. The coalition formation process is a result of Pareto order agreements for merge (or split) between the users. For example, in DF, coalition $\{5, 8, 10, 13\}$ formed since all the users agree on its formation due to the fact that $V(\{5, 8, 10, 13\}) = \{\boldsymbol{\phi}(\{5, 8, 10, 13\}) = [0.356\ 0.8952\ 1.7235\ 0.6213]\}$ which is a clear improvement on the non-cooperative utility which was 0 for all four users (due to proximity to eavesdropper 2). For AF, Fig. 2 shows that only users $\{5, 8, 13\}$ and users $\{1, 6, 7, 10\}$ cooperate while all others remain non-cooperative. The main reason is that, in AF, the users need to amplify a noisy version of the signal using the beamforming weights. As a consequence, the noise can be highly amplified, and, for AF, cooperation is only beneficial in very favorable conditions. For example, coalitions $\{5, 8, 13\}$ and $\{1, 6, 7, 10\}$ have formed for AF due to being far from the eavesdroppers (relatively

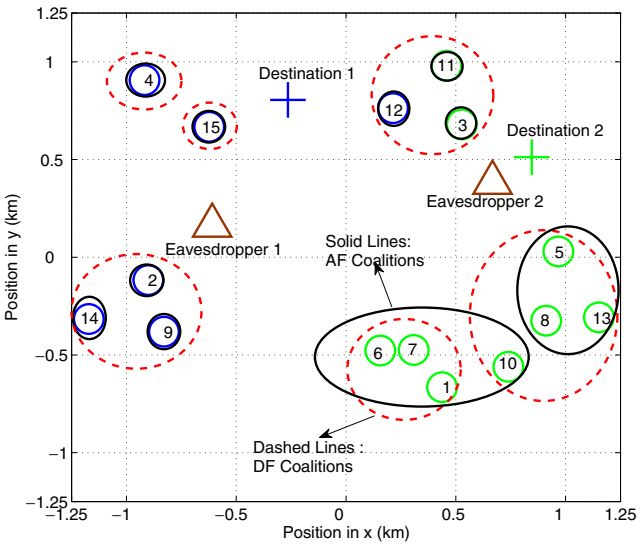

Fig. 2 A snapshot of a coalitional structure resulting from our proposed coalition formation algorithm for a network with $N = 15$ users, $M = 2$ destinations and $K = 2$ eavedroppers for DF (*dashed lines*) and AF (*solid lines*)

[1] This general network setting captures a broad range of network types ranging from ad hoc networks, to sensor networks, WLAN networks as well as broadband or cellular networks.

to the other users), hence, having a small cost for information exchange. In contrast, for coalitions such as {3, 11, 12}, the benefit from cooperation using AF is small compared to the cost, and, thus, these coalitions do not form.

In Fig. 3 we show how the algorithm handles mobility through appropriate coalition formation decisions. For this purpose, the network setup of Fig. 2 is considered for the DF case while User 12 is moving horizontally with a constant speed of 10 km/h for a period of 6.6 min, hence, up to 1.1 km in the direction of the *negative* x-axis. First of all, User 12 starts getting closer to its receiver (destination 2), and, hence, it improves its utility. In the meantime, the utilities of User 12's partners (Users 3 and 11) drop due to the increasing cost. As long as the distance covered by User 12 is less than 0.2 km, the coalition of Users 3, 11 and 12 can still bring mutual benefits to all three users. After that, splitting occurs by a mutual agreement and all three users transmit independently. When User 12 moves about 0.8 km, it begins to distance itself from its receiver and its utility begins to decrease. When the distance covered by User 12 reaches about 1 km, it will be beneficial to Users 12, 4, and 15 to form a 3-user coalition through the merge rule since they improve their utilities from $\phi_4(\{4\}) = 0.2577$, $\phi_{12}(\{12\}) = 0.7638$, and $\phi_{15}(\{15\}) = 0$ in a non-cooperative manner to $V(\{4, 12, 15\}) = \{\boldsymbol{\phi}(\{4, 12, 15\}) = [1.7618\ 1.0169\ 0.6227]\}$.

In Fig. 4 we show the performance, in terms of average utility (secrecy rate) per user, as a function of the network size N for both the DF and AF cases for

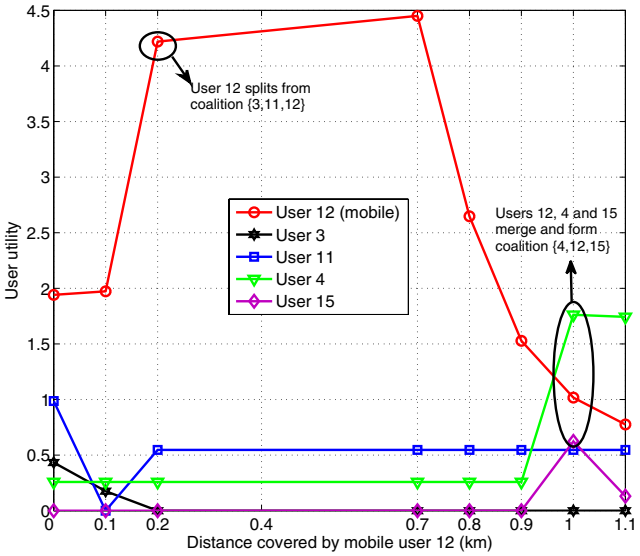

Fig. 3 Self-adaptation of the network's topology to mobility as User 12 in Fig. 2 moves horizontally on the negative x-axis (for DF)

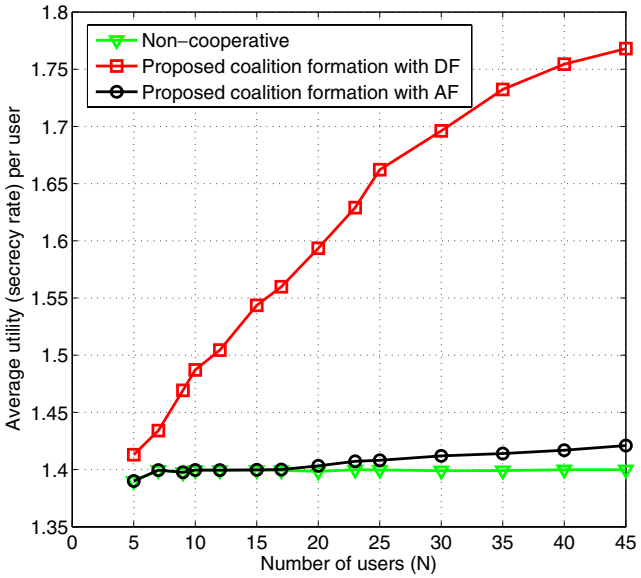

Fig. 4 Performance in terms of the average individual user utility (secrecy rate) as a function of the network size N for $M = 2$ destinations and $K = 2$ eavesdroppers

a network with $K = 2$ eavesdroppers. First, we note that the performance of coalition formation with DF is increasing with the size of the network, while the non-cooperative and the AF case present an almost constant performance. For instance, for the DF case, Fig. 4 shows that, by forming coalitions, the average individual utility (secrecy rate) per user is increased at all network sizes with the performance advantage of DF increasing with the network size and reaching up to 25.3 and 24.4% improvement over the non-cooperative and the AF cases, respectively, at $N = 45$. This is interpreted by the fact that, as the number of users N increases, the probability of finding candidate partners to form coalitions with, using DF, increases for every user. Moreover, Fig. 4 shows that the performance of AF cooperation is comparable to the non-cooperative case. Hence, although AF relaying can improve the secrecy rate of large clusters of nearby cooperating users when no cost is accounted for such as in [10], in a practical wireless network and in the presence of a cooperation cost, the possibility of cooperation using AF for secrecy rate improvement is rare as demonstrated in Fig. 4. This is mainly due to the strong dependence of the secrecy rate for AF cooperation on the channel between the users as per Eq. 5, as well as the fact that, for AF, unless highly favorable conditions exist (e.g. for coalitions such as {1, 6, 7, 10} in Fig. 2) , the amplification of the noise resulting from beamforming using AF relaying hinders the gains from cooperation relative to the secrecy cost during the information exchange phase.

In Fig. 5, we show the performance, in terms of average utility (secrecy rate) per user, as the number of eavesdroppers K increases for both the DF and AF cases for a network with $N = 45$ users. Figure 4 shows that, for DF, AF and the non-cooperative case, the average secrecy rate per user decreases as more eavesdroppers are present in the area. Moreover, for DF, the proposed coalition formation algorithm presents a performance advantage over both the non-cooperative case and the AF case at all K. Nonetheless, as shown by Fig. 5, as the number of eavesdroppers increases, it becomes quite difficult for the users to improve their secrecy rate through coalition formation; consequently, at $K = 8$, all three schemes exhibit a similar performance. Finally, similar to the results of Fig. 4, coalition formation using the AF cooperation protocol has a comparable performance with that of the non-cooperative case at all K as seen in Fig. 5.

In Fig. 6, for DF cooperation, we show the average and average maximum coalition size resulting from the proposed algorithm as the number of users, N, increases, for a network with $K = 2$ eavesdroppers. Figure 6 shows that both the average and average maximum coalition size increase with the number of users. This is mainly due to the fact that as N increases, the number of candidate cooperating partners increases. Further, through Fig. 6 we note that the formed coalitions have a small average size and a relatively large maximum size reaching up to around 2 and 6, respectively, at $N = 45$. Since the average coalition size is below the minimum of 3 (as per Remark 1 due to having 2 eavesdroppers) and the average maximum coalition size is relatively large, the network structure is thus composed of a number of large coalitions with a few non-cooperative users.

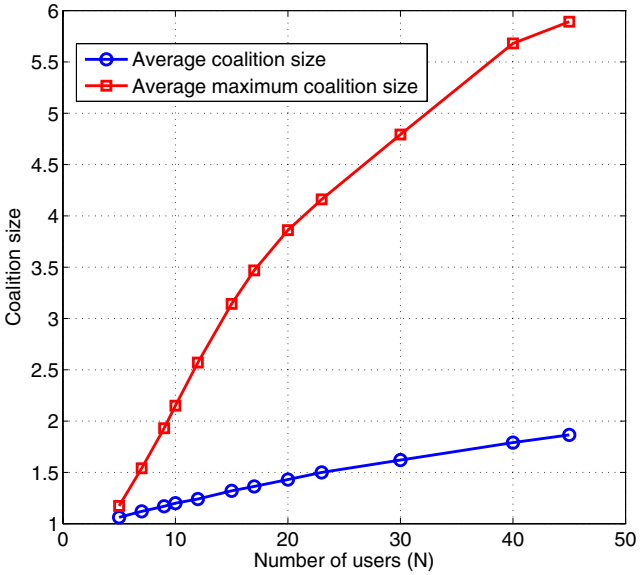

Fig. 6 Average and average maximum coalition size as the network size N varies for $M = 2$ destinations and $K = 2$ eavesdroppers and DF cooperation

Figure 7 shows the average (averaged over the random positions of the users, eavesdroppers, and des-

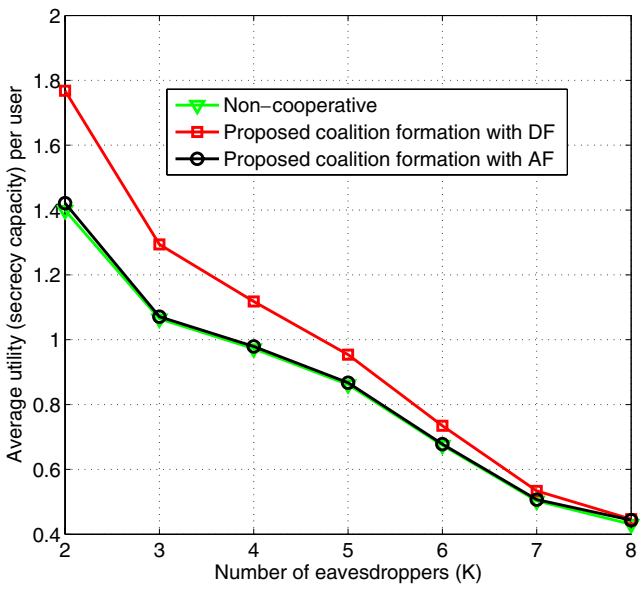

Fig. 5 Performance in terms of the average individual user utility (secrecy rate) as a function of the number of eavesdroppers K for $N = 45$ users and $M = 2$ destinations

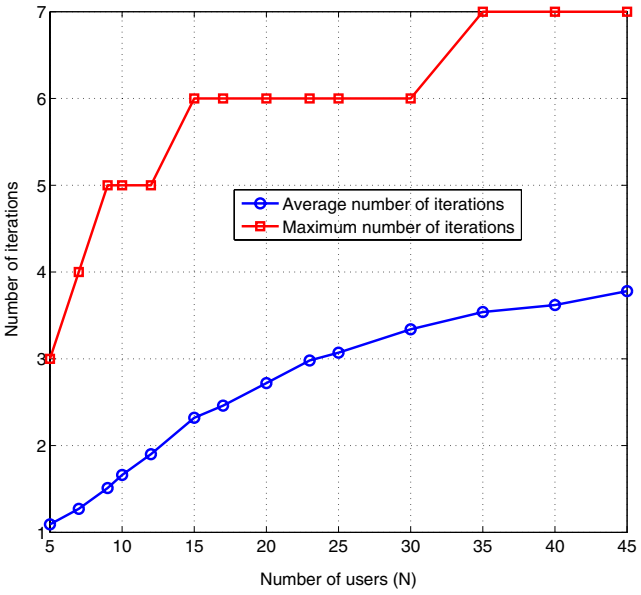

Fig. 7 Average and maximum number of iterations as the network size N varies for for a network $M = 2$ destinations and $K = 2$ eavesdroppers and DF cooperation

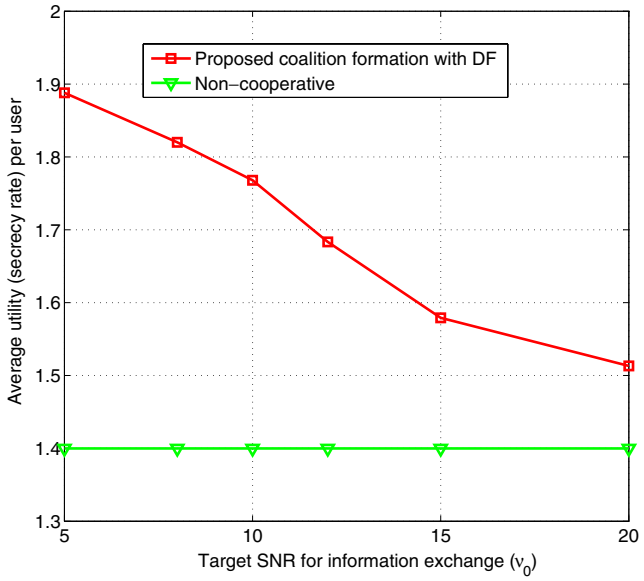

Fig. 8 Average individual user utility as a function of the target SNR v_0 for information exchange for a network with $N = 45$ users, $K = 2$ eavesdroppers and $M = 2$ destinations for DF

tinations) and maximum number of merge-and-split iterations that occur prior to the convergence of the proposed algorithm as the number of users, N, increases, for a network with $K = 2$ eavesdroppers and $M = 2$ destinations with DF cooperation. In Fig. 7, we can see that the average and maximum number of iterations increases with the network size. This is mainly due to the fact that as N increases, the possibilities for cooperation increase, yielding an increased number of merge-and-split iterations. In this figure, we remark the the average and maximum number of merge-and-split iterations required for the convergence vary, respectively, from 1.1 and 3 at $N = 5$ to around 3.8 and 7 at $N = 45$ users. Roughly, this result implies that for a network of $N = 45$ RSUs an average of about 4 merge-and-split iterations are required before convergence, which demonstrates that the convergence time of the proposed algorithm is quite reasonable.

In Fig. 8, the performance, in terms of average utility (secrecy rate) per user, of the network for different cooperation costs, i.e., target average SNRs v_0 is assessed. Figure 8 shows that cooperation through coalition formation with DF maintains gains, in terms of average secrecy rate per user, at almost all costs (all SNR values). However, as the cost increases and the required target SNR becomes more stringent these gains decrease converging further towards the non-cooperative gains at high cost since cooperation becomes difficult due to the cost. As seen in Fig. 8, the secrecy rate gains resulting from the proposed coalition formation algorithm range from 8.1% at $v_0 = 20$ dB to around 34.9% at $v_0 = 5$ dB improvement relative to the non-cooperative case.

The proposed algorithm's performance is further investigated in networks with $N = 20$ and $N = 45$ *mobile* users for a period of 5 min in the presence of $K = 2$ stationary eavesdroppers. We adopt a basic random walk mode whereby the nodes move at a constant speed in a random direction uniformly distributed between 0 and 2π, over periods of 30 s. Also, during this period, the proposed algorithm is run periodically every 30 s as well. The results in terms of the frequency of merge and split operations per minute are shown in Fig. 9 for various speeds. As the speed increases, the frequency of both merge and split operations per minute increases due to the changes in the network structure incurred by the increased mobility. These frequencies reach up to around 19 merge operations per minute and 9 split operations per minute for $N = 45$ at a speed of 72 km/h. Finally, Fig. 9 demonstrates that the frequency of merge and split operations increases with the network size N as the users become more apt to finding new cooperation partners when moving which results in an increased coalition formation activity.

Figure 10 shows, for DF, how the structure of the wireless network with $N = 45$ users and $K = 2$ mobile eavesdroppers evolves and self-adapts over time (a period of 5 min), while both eavesdroppers are mobile

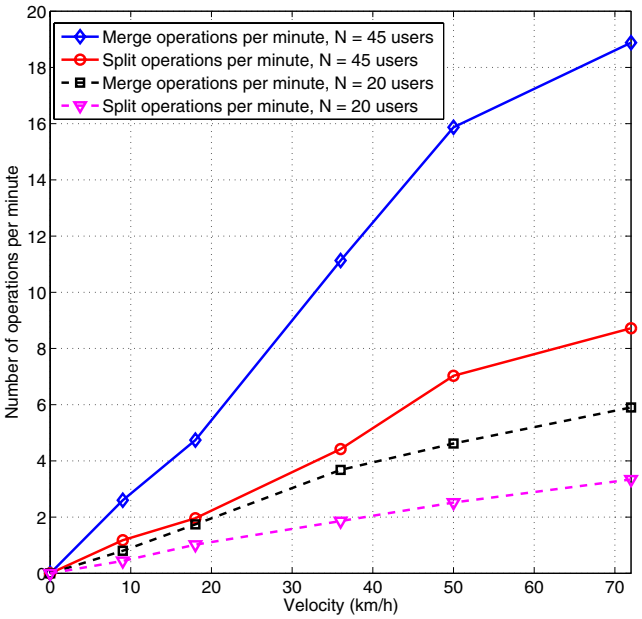

Fig. 9 Frequency of merge and split operations per minute vs. speed of the users for different network sizes and $K = 2$ eavesdroppers with DF cooperation

with a constant velocity of 50 km/h (similar random walk mobility of Fig. 9). The proposed coalition formation algorithm is repeated periodically by the users every 30 s, in order to provide self-adaptation to mobility. First, the users self-organize into 22 coalitions after the occurrence of 10 merge and split operations at time $t = 0$. As time evolves, through adequate merge and split operations the network structure is adapted to the mobility of eavesdroppers. For example, at time $t = 1$ min, through a total of 6 operations constituted of 5 merge and 1 split, the network structure changes from a partition of 26 coalitions back to a partition of 22 coalitions. Further, at $t = 3$ min, no merge or split operations occur, and, thus, the network structure remain unchanged. In summary, Fig. 10 illustrates how the users can take adequate merge or split decisions to adapt the network structure to the mobility of the eavesdroppers.

In order to assess the impact of the users-destination assignment scheme on the performance, in Fig. 11, we show the average utility (secrecy rate) per user, as a function of the network size N for both the DF and AF cases for a network with $K = 2$ eavesdroppers when the users are *randomly* assigned to their destinations. First, compared with Fig. 4, we can see that, by randomly assigning the users to their destinations, the average utility per user resulting from both the cooperative (DF and AF) and non-cooperative cases is smaller than that achieved when the users are assigned to their closest destination. The main reason behind this result is that,

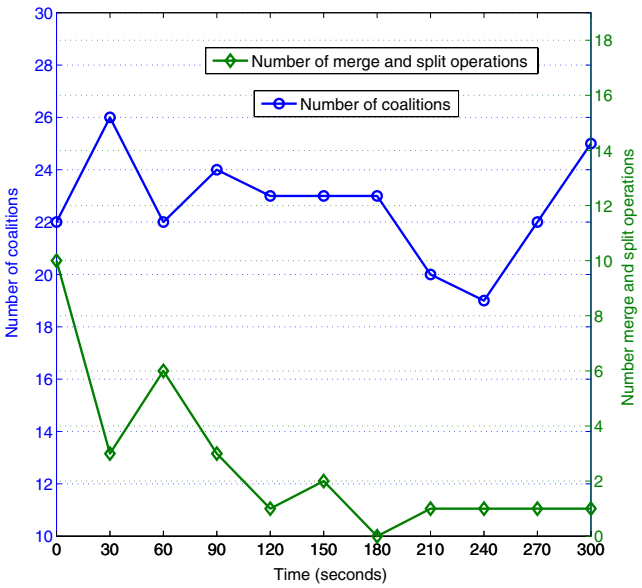

Fig. 10 Evolution over time for a network with $N = 45$ users, $M = 2$ destinations, and $K = 2$ eavesdroppers with DF cooperation when the eavesdroppers are moving with a speed of 50 km/h

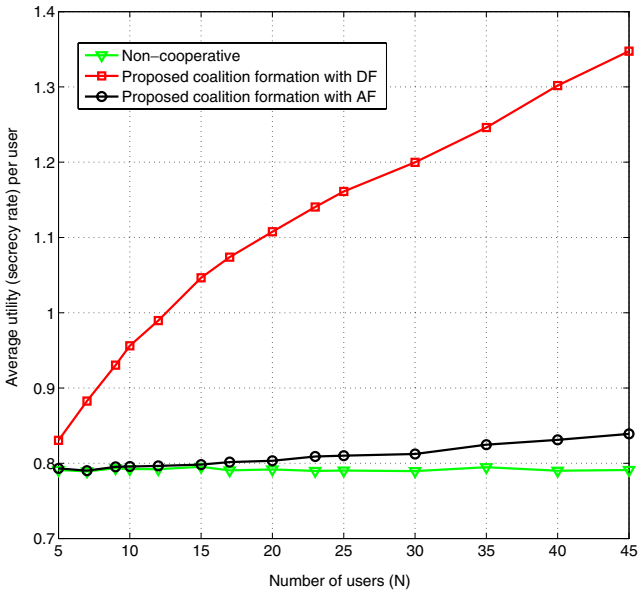

Fig. 11 Performance in terms of the average individual user utility (secrecy rate) as a function of the network size N for $M = 2$ destinations and $K = 2$ eavesdroppers when the users are assigned *randomly* to their destinations

when assigned to their closest destination, the users have a better channel as per the considered channel model, and, thus, their resulting secrecy rates are better. Nonetheless, Fig. 11 demonstrates that, when the users are assigned randomly to their destination, the advantage of coalition formation is significantly higher than in the case of Fig. 4. For instance, for the DF case, Fig. 11 shows that the performance advantage of coalition formation with DF reaches up to 70.3 and 60.6% improvement over the non-cooperative and the AF cases, respectively, at $N = 45$. Moreover, even with the AF case, Fig. 11 shows that up to 6% of improvement relatively to the non-cooperative case is also possible at $N = 45$ users, which is better than the performance of AF in Fig. 4. Hence, Fig. 11 clearly shows that, even with a random assignment of the users to their destination, the proposed coalition formation algorithm can yield significant gains compared to the non-cooperative case, notably with DF cooperation.

6 Conclusions

In this paper, we have studied the user behavior, topology, and dynamics of a network of users that interact in order to improve their secrecy rate through both decode-and-forward and amplify-and-forward cooperation. We formulated the problem as a non-transferable

coalitional game, and proposed a distributed and adaptive coalition formation algorithm. Through the proposed algorithm, the mobile users are able to take a distributed decision to form or break cooperative coalitions through well suited rules from cooperative games while maximizing their secrecy rate taking into account various costs for information exchange. We have characterized the network structure resulting from the proposed algorithm, studied its stability, and analyzed the self-adaptation of the topology to environmental changes such as mobility. Simulation results have shown that, for decode-and-forward, the proposed algorithm allowed the users to self-organize while improving the average secrecy rate per user up to 25.3 and 24.4% (for a network with 45 users) relative to the non-cooperative and amplify-and-forward cases, respectively.

References

1. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387
2. Leung-Yan-Cheong SK, Hellman, ME (1978) The Gaussian wiretap channel. IEEE Trans Inf Theory 24(4):451–456
3. Csiszar I, Korner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24(3):339–348
4. Liang Y, Poor HV, Shamai S (2008) Secure communication over fading channels. IEEE Trans Inf Theory 54(6):2470–2492
5. Gopala PK, Lai L, Gamal HE (2008) On the secrecy capacity of fading channels. IEEE Trans Inf Theory 54(10):4687–4698
6. Liang Y, Poor HV (2008) Multiple-access channels with confidential messages. IEEE Trans Inf Theory 54(3):976–1002
7. Prada P, Blahut R (2005) Secrecy capacity of SIMO and slow fading channels. In: Proc. int. symp. inf. theory. Adelaide, Australia, pp 2152–2155
8. Li Z, Trappe W, Yates R (2007) Secret communication via multi-antenna transmission. In: Proc. of 41st conference on information sciences and systems. Baltimore, MD
9. Dong L, Han Z, Petropulu A, Poor HV (2008) Secure wireless communications via cooperation. In: Proc. Allerton conference on communication, control, and computing. Monticello, IL
10. Dong L, Han Z, Petropulu A, Poor HV (2009) Amplify-and-forward based cooperation for secure wireless communication. In: Proc. international conf. on acoustics, speech, and signal processing. Taipei, Taiwan
11. Han Z, Marina N, Debbah M, Hjørungnes A (2009) Physical layer security game: Interaction between source, eavesdropper and friendly jammer. EURASIP Journal on Wireless Communications and Networking, vol 2009
12. Saad W, Han Z, Debbah M, Hjørungnes A, Başar T (2009) Coalition game theory for communication networks: a tutorial. IEEE Signal Process Mag (special issue on Game Theory in Signal Processing and Communications) 26(5):77–97
13. Proakis J (2001) Digital communications, 4th edn. McGraw-Hill, New York
14. Liang Y, Kramer G, Poor HV, Shamai S (2007) Compound wire-tap channels. In: Proc. Allerton conference on communication, control, and computing. Monticello, IL
15. Jindal N, Mitra U, Goldsmith A (2004) Capacity of ad-hoc networks with node cooperation. In: Proc. int. symp. on information theory. Chicago, IL, p 271
16. Vishwanathan H, Venkatesa S, Huang H (2003) Downlink capacity evaluation of cellular networks with known interference cancellation. IEEE J Sel Areas Commun 21(5):802–811
17. Saad W, Han Z, Debbah M, Hjørungnes A (2008) A distributed merge and split algorithm for fair cooperation in wireless networks. In: Proc. int. conf. on communications, workshop on cooperative communications and networking. Beijing, China
18. Kramer G, Maric I, Yates RD (2007) Cooperative communications. Now Publishers Inc.
19. Maham B, Hjørungnes A, Abreu G (2009) Distributed GABBA space-time codes in amplify-and-forward relay networks. IEEE Trans Wirel Commun 8(4):2036–2045
20. Myerson RB (1991) Game theory, analysis of conflict. Harvard University Press, Cambridge
21. Ray D (2007) A game-theoretic perspective on coalition formation. Oxford University Press, New York
22. Apt K, Witzel A (2006) A generic approach to coalition formation. In: Proc. of the int. workshop on computational social choice (COMSOC). Amsterdam, the Netherlands
23. Han Z, Liu KJR (2008) Resource allocation for wireless networks: basics, techniques, and applications. Cambridge University Press
24. Li XY (2008) Wirless ad hoc and sensor networks: theory and applications. Cambridge University Press, Cambridge
25. Saad W, Han Z, Başar T, Debbah M, Hjørungnes A (2009) Physical layer security: Coalitional games for distributed cooperation. In: Proc. 7th int. symp. on modeling and optimization in mobile, ad hoc, and wireless networks (WiOpt). Seoul, South Korea