Coalitional Games for Distributed Eavesdroppers Cooperation in Wireless Networks

Walid Saad, Han Zhu, Tamer Basar, Merouane Debbah, Are Hjorungnes

Coalitional Games for Distributed Eavesdroppers Cooperation in Wireless Networks

Walid Saad
UNIK - University Graduate Center
University of Oslo
Kjeller, Norway
saad@unik.no

Zhu Han
Electrical and Computer Engineering Department
University of Houston
Houston, USA
zhan2@mail.uh.edu

Tamer Başar
Coordinated Science Laboratory
University of Illinois
Urbana-Champaign, USA
basar1@illinois.edu

Mérouane Debbah
Alcatel-Lucent Chair
SUPELEC
Paris, France
merouane.debbah@supelec.fr

Are Hjørungnes
UNIK - University Graduate Center
University of Oslo
Kjeller, Norway
arehj@unik.no

ABSTRACT

Physical layer security aspects of wireless networks have recently attracted an increased attention due to the emergence of large-scale decentralized networks. While most existing literature focuses on link-level performance analysis from the perspective of the wireless users, this paper turns the attention to the eavesdroppers' (attacker) side of the problem. In this context, we introduce a model that enables a number of single antenna eavesdroppers in a wireless network to cooperate, by performing distributed receive beamforming, for improving the damage that they inflict on the network's wireless users when tapping through their transmissions. We model the eavesdroppers cooperation problem as a non-transferable coalitional game and we propose a distributed algorithm for coalition formation. The proposed algorithm allows the eavesdroppers to take autonomous decisions to cooperate and form coalitions, while maximizing the damage that they cause on the wireless users. This damage is quantified in terms of the overall secrecy capacity reduction that the eavesdroppers incur on the users while taking into account cooperation costs in terms of the time required for information exchange. We analyze the resulting coalitional structures, discuss their properties, and study how the eavesdroppers can adapt the topology to environmental changes such as mobility. Simulation results show that the proposed algorithm allows the eavesdroppers to cooperate and self-organize while achieving an improvement of the average payoff per eavesdropper up to 27.6% per eavesdropping cycle relative to the non-cooperative case.

*This work was done 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 projects 183311/S10, 176773/S10, and 18778/V11.

1. INTRODUCTION

In recent years, there has been an increased interest in the physical layer (PHY) security aspects of wireless networks. The main motivation is that higher-layer techniques, such as encryption, are too complex and hard to implement in decentralized and large-scale wireless networks. Hence, the study of the PHY security of these networks has become of major interest. The main idea is to study the wireless channel PHY characteristics and their implications on the reliability and security of wireless transmission which is quantified using the *secrecy capacity*. The secrecy capacity is defined as the maximum rate of secret information sent from a node to its destination in the presence of eavesdroppers. The study of this security aspect began with pioneering work of Wyner over the wire-tap channel [1] which showed the possibility of having an almost perfectly secure communication without any reliance on secret keys. This work was followed up in [2, 3] for the scalar Gaussian wire-tap channel and the broadcast channel, respectively.

A significant amount of research has been recently devoted to carrying out these PHY security studies unto the wireless and the multi-user channels [4–9]. 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. For improving the users' secrecy capacities, multiple antenna systems have been proposed in [7, 8], notably when the channel between the source and the destination is worse than the channel between the source and the eavesdroppers. Further, the possibility of benefiting from these multiple antenna gains is studied in [9] and [10] through cooperation among the users. Briefly, the majority of the existing literature is devoted to the information theoretic analysis, from the perspective of the network's *users*, of link-level performance gains of secure communications.

However, there is a lack of literature that studies how the eavesdroppers can behave for improving their eavesdropping capabilities, notably at the system-level. In fact, to the best of our knowledge, no work has investigated how a number of eavesdroppers can interact at the network-wide level in order to launch efficient eavesdropping attacks on a network of wireless users.

The main contributions of this work are three-fold: (i) To introduce a cooperation protocol that allows a network of eavesdroppers to interact for improving their eavesdropping performance, (ii) To propose an adequate utility function for the eavesdroppers that accounts for the cooperation gains and costs, and (iii) To model the problem using coalitional games and introduce a distributed algorithm for coalition formation among the eavesdroppers. In other words, while existing work focused mainly on the users' side in PHY security problems, we seek to study the eavesdroppers' perspective while proposing cooperative strategies. For this purpose, we model the eavesdroppers cooperation problem as a non-transferable coalitional game and we propose an algorithm for distributed coalition formation constructed using well suited concepts from cooperative games. Using the proposed algorithm, the eavesdroppers in a wireless network can autonomously decide to form or break a coalition for maximizing their utilities. These utilities account for the gain from cooperation, in terms of the average reduction of the overall secrecy capacity incurred on the users (damage caused by the eavesdroppers) as well as the costs in terms of the time needed for information exchange among the eavesdroppers. We show that, due to the cost for cooperation, independent disjoint eavesdroppers coalitions will form in the network. We study and discuss the properties of these resulting coalitional structures. Simulation results show that the proposed algorithm allows the eavesdroppers to cooperate and self-organize while achieving an improvement of the average payoff (overall secrecy capacity reduction) per eavesdropper up to 27.6% per eavesdropping cycle relative to the non-cooperative case. The simulations also show how the eavesdroppers can adapt the network's topology to environmental changes such as mobility.

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

2.1 Non-Cooperative Eavesdropping Model

Consider a network having K single antenna eavesdroppers (static or mobile) seeking to tap into the transmissions of N wireless transmitters that are sending data to a central base station (BS). Denote $\mathcal{K}$ and $\mathcal{N}$ as the sets of eavesdroppers and users, respectively. We consider that each eavesdropper can only eavesdrop on one user at a time[1]. In a non-cooperative manner, we consider that, at any given point in time, all K eavesdroppers are interested in the information being sent by only one user $i \in \mathcal{N}$. Hence, we consider a time slotted system whereby during a single slot all K eavesdroppers, each acting on its own (non-cooperatively), attempt to tap into the transmission of *one* of the N users in the network[2]. The eavesdroppers can attack the users in any arbitrary manner over the slots. Due to the non-cooperative and independent behavior of these attacks (which are also ergodic over time), this model can be captured, for convenience, by a round robin system operation. Hence, in slot 1, we consider that all eavesdroppers are non-cooperatively attacking User 1, in slot 2, all eavesdroppers are non-cooperatively attacking User 2, and so on until all N users are attacked once by the eavesdroppers. Consequently, a total of N slots is required for completing one round of eavesdropping on all N users. Every block of N slots will be referred to as the *eavesdropping cycle* and the eavesdroppers engage in multiple eavesdropping cycles over time.

Moreover, as the wireless channel is time varying, the duration of every time slot is considered to be equal to the coherence time θ_c of the channel (assumed to be the same for all channels in the model) which is defined as the time during which the channel is considered as invariant. Hence, within a slot, the eavesdroppers can launch an attack knowing that the channels do not vary during the slot. The coherence time is generally given by [11, Eq. (4.40.c)]

$$\theta_c = \frac{0.423}{f_d} \tag{1}$$

where f_d is the maximal Doppler frequency (for stationary eavesdroppers/users this frequency has a value of a few hertz and can increase with increased mobility [11, Sec. 4.4.3]).

During a single eavesdropping cycle (N slots), the objective of every eavesdropper is to maximize the damage caused on the users, which translates into minimizing the secrecy capacities of all N users (during one cycle). In this regard, the total damage that an eavesdropper $k \in \mathcal{K}$ is able to inflict on the transmitters through a single eavesdropping cycle can be quantified using the *overall reduction of the secrecy capacities* that k yielded, as follows

$$u(k) = \sum_{i \in \mathcal{N}} \left(C_i^d - C_{k,i}^e \right)^+, \tag{2}$$

where $C_i^d = W \cdot \log_2 \left(1 + \frac{g_{i,\mathrm{BS}}^2 \cdot \tilde{P}}{\sigma^2}\right)$ is the capacity of user $i \in \mathcal{N}$ achieved at the BS with $g_{i,BS}$ being the channel gain between i and the BS, W being the available bandwidth, $\tilde{P}$ being the transmit power of user i (assumed the same for all users in $\mathcal{N}$), and σ^2 the variance of the Gaussian noise. Further, $C_{k,i}^e = W \cdot \log_2 \left(1 + \frac{g_{i,k}^2 \cdot \tilde{P}}{\sigma^2}\right)$ is the capacity received at eavesdropper k from user i. In this paper, we consider a quasi-static channel model where the channel gain $g_{i,j}$ between any two nodes (users-base station, eavesdropper-user, or eavesdropper-eavesdropper) is given by [11]

$$g_{i,j} = a \cdot \sqrt{d_{i,j}^{-\mu}} \tag{3}$$

[1]Simultaneous eavesdropping by a single eavesdropper on multiples users requires complex computational and signal processing techniques that are hard to integrate namely when the eavesdroppers are small mobile devices and the number of users is large.

[2]This model is selected without loss of generality since our analysis and algorithm can easily accommodate the case where each eavesdropper may select a different user to tap into within a slot.

where $d_{i,j}$ is the distance between nodes i and j, μ the path loss exponent, and a is a Rayleigh distributed fading amplitude with a variance of 1 which is stable over the duration of a slot but changes from one slot to the other (quasi-static channel).

Further, we remark that in (2) every element $(C_i^d - C_{k,i}^e)^+$ of the summation represents the secrecy capacity that user $i \in \mathcal{N}$ achieves when its signal is being tapped into by eavesdropper k. Hence, each element of the summation quantifies the damage that eavesdropper k is able to cause on user i when tapping into its signal during the corresponding time slot. The eavesdroppers aim at minimizing the summation in (2) in every eavesdropping cycle by maximizing the damage caused through the eavesdropping capacities $C_{k,i}^e, \forall k \in \mathcal{K},\ i \in \mathcal{N}$. Due to the fading and path loss of the eavesdropper-user channel, these eavesdropping capacities may be small, thus, reducing the overall effectiveness of the eavesdropping process of all eavesdroppers. Hence, efficient techniques for combatting this fading is needed by the eavesdroppers in order to improve their performance.

2.2 Cooperative Eavesdropping Model

Recently, distributed cooperation among single antenna wireless nodes has been proposed [9, 12, 13] as an effective mean for improving the quality of the transmitted or received signal by exploiting spatial diversity. A key technique in this area is collaborative beamforming whereby the radio signals transmitted from (transmit beamforming) or received by (receive beamforming) a set of single-antenna users with non-directional antennas can be combined using advanced signal processing techniques for improving the performance (capacity, signal-to-noise ratio, etc.) of the wireless system by cooperatively directing the antenna beam [13–17].

In this context, for improving their performance in terms of eavesdropping capacities, the eavesdroppers in our model can cooperate by forming groups of eavesdroppers known as coalitions. Within every coalition, the eavesdroppers utilize collaborative receive beamforming techniques for minimizing the secrecy capacities achieved by the users through an increase in the eavesdropping capacities achieved. Thus, every coalition $S \subseteq \mathcal{K}$ can be seen as a single eavesdropper with multiple receive antennas and, within a single slot, this coalition can collaboratively tap into the signal of one of the users. For every coalition S, a two-stage cooperation protocol is proposed whereby the coalition divides its slot into two durations as follows (this protocol is used every slot to eavesdrop on a particular user $i \in \mathcal{N}$):

1. In a first duration of the slot, each eavesdropper k broadcasts its information (channel, control, etc.) to the other members of coalition S. This is the information exchange stage which is performed sequentially by the eavesdroppers in S.

2. In the remaining time of the slot, the members of coalition S engage in cooperative receive beamforming, i.e., the coalition directs its beam towards user i that is currently being tapped into.

Consequently, analogous to the non-cooperative network operation, in a cooperative manner, during an eavesdropping cycle, each time slot, all the coalitions (each coalition acting on its own) eavesdrop on one user $i \in \mathcal{N}$ in a round robin manner. An illustrative example of the network operation in the cooperative and non-cooperative case is shown in Fig. 1 for $K = 8$ eavesdroppers, $N = 5$ users, and 3 coalitions.

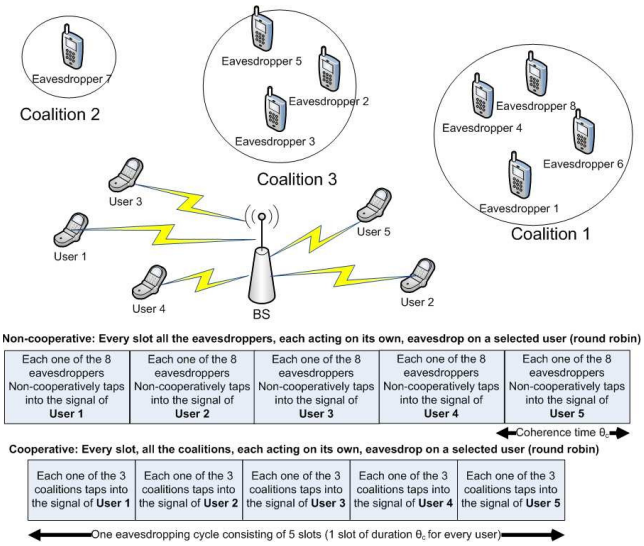

Figure 1: An illustrative example of the proposed system model for eavesdroppers cooperation.

For performing receive beamforming, it is well known [12] that the optimal SNR maximizing technique for combining the received signals and directing the beam towards a particular direction is through maximal ratio combining (MRC) [14]. Hence, within every coalition, the eavesdroppers perform MRC for maximizing the SNR received from the users, consequently reducing the secrecy capacities of these users. In this regard, the eavesdropping capacity $C_{S,i}^e$ of a coalition $S \subseteq \mathcal{K}$ which performs MRC receive beamforming while tapping into the signal of user $i \in \mathcal{N}$ is given by [12, 15, 16]

$$C_{S,i}^e = W \cdot \log_2 \left(1 + \frac{\tilde{P} \cdot \|\boldsymbol{h}\|^2}{\sigma^2}\right) \tag{4}$$

where $\boldsymbol{h}$ is the $|S| \times 1$ channel vector, where each row element $h_k = g_{i,k}$ with $g_{i,k}$ the channel gain between user i and eavesdropper $k \in S$ as given by (3). By achieving the eavesdropping capacity of (4), the eavesdroppers can certainly improve the damage incurred on the users as clearly seen by combining (4) with (2).

However, during the first stage of the cooperation protocol, i.e., the information exchange stage between the eavesdroppers, the users are able to transmit securely without being overheard by the eavesdroppers since the eavesdroppers are engaged in exchanging their channel and control information. Thus, the information exchange time yields a cost for cooperation on the eavesdroppers, in terms of security, since the users are able to securely communicate in this period. Moreover, during this first duration, the users can overhear the information exchange among the eavesdroppers (act as eavesdroppers on the eavesdroppers!) and, thus, detect the presence of the eavesdropping threat which also constitutes a cost for cooperation that the eavesdroppers must account for when evaluating the effectiveness of their attack through (2) and (4).

Accordingly, consider a coalition S that is operating to eaves-

drop on a user $i \in \mathcal{N}$ during a given slot. Within the first duration of the slot every eavesdropper $k \in S$ exchanges its information with the members of S by sending its data to the farthest member $\hat{k} = \arg\max_{l \in S}(d_{k,l})$ in S as the other members of S can simultaneously receive this information due to the broadcast nature of the wireless channel. Due to the possibility that the users may tap into the information exchange of the eavesdroppers, the rate at which an eavesdropper $k \in S$ exchanges its information is the secrecy capacity achieved by k while user i (the user being targeted by S in the slot) is considered as an eavesdropper which is given by

$$C^{\text{exch}}_{k,\hat{k},i} = \left(C_{k,\hat{k}} - C^{e}_{i,k}\right)^{+}, \tag{5}$$

where $C_{k,\hat{k}} = W \cdot \log_2\left(1 + \frac{P_{k,\hat{k}} \cdot g^2_{k,\hat{k}}}{\sigma^2}\right)$ is the transmit capacity for information exchange between eavesdropper k and the farthest eavesdropper $\hat{k}$ with $P_{k,\hat{k}}$ the transmit power of eavesdropper k, and $C^{e}_{i,k} = W \cdot \log_2\left(1 + \frac{P_{k,\hat{k}} \cdot g^2_{k,i}}{\sigma^2}\right)$ is the capacity with which user i is able to tap into the information exchange transmission between the eavesdroppers. Without any loss of generality, we assume $P_{k,\hat{k}} = \tilde{P}, \forall k \in \mathcal{K}$.

By using (5) we can deduce the fraction of time θ^i_k required for information exchange (without being tapped into by transmitter $i \in \mathcal{N}$) between an eavesdropper $k \in S$ and the other members of coalition S (applicable to the slot when the coalition's beam is directed towards user i) as follows

$$\theta^i_k = \left(\frac{\theta^i_{k,\hat{k}}}{\theta_c}\right), \tag{6}$$

where θ_c is the coherence time given by (1) and

$$\theta^i_{k,\hat{k}} = \frac{L}{C^{\text{exch}}_{k,\hat{k},i}} \tag{7}$$

is the time it takes for eavesdropper $k \in S$ to send a packet of L bits (containing channel, control, and cooperation information) to the farthest eavesdropper $\hat{k} \in S$, i.e., exchange information with the other members of S, with $C^{\text{exch}}_{k,\hat{k},i}$ given by (5). Hence, as the eavesdroppers in S exchange their data sequentially, the total time consumed by coalition S for information exchange when eavesdropping on user i is

$$\theta_{S,i} = \left(\sum_{k \in S} \theta^i_{k,\hat{k}}\right)^{-}, \tag{8}$$

with $a^{-} \triangleq \min(a, 1)$. Clearly, the cost $\theta_{S,i}$ accounts for both types of cooperation costs previously mentioned: (i) The time for information exchange during which users are transmitting securely as well as (ii) The possibility that the users may overhear the transmission between the eavesdroppers during information exchange.

Given the cost $\theta_{S,i}$, the total secrecy capacity reduction that a coalition S can cause on the users during an eavesdropping cycle can be given by

$$u(S) = \sum_{i \in \mathcal{N}} \left(\theta_{S,i} \cdot C^d_i + (1 - \theta_{S,i})\left(C^d_i - C^e_{S,i}\right)^{+}\right), \tag{9}$$

where $C^e_{S,i}$ is the receive beamforming eavesdropping capacity given in (4) and $\theta_{S,i}$ the time cost given in (8). Note that, if S is a singleton, then $u(S)$ reduces to the expression given in (2) (for a singleton coalition of size 1 there is no information exchange, i.e., $\theta_{S,i} = 0$). Every element in the summation of (9) represents the secrecy capacity reduction for the slot where S was eavesdropping on a user $i \in \mathcal{N}$ using the two stage cooperative protocol previously proposed. For instance, during the eavesdroppers information exchange $\theta_{S,i}$ duration, user i is able to transmit freely with no eavesdropping, hence the term $\theta_{S,i} \cdot C^d_i$. For the remaining slot duration $(1 - \theta_{S,i})$, coalition S is able to eavesdrop on user i with an improved performance due to the receive beamforming gain as exhibited by $C^e_{S,i}$ in the term $(1 - \theta_{S,i})\left(C^d_i - C^e_{S,i}\right)^{+}$. The objective of the eavesdroppers (coalitions) is to minimize (9), hence, maximizing the damage on the users.

For a better understanding of (9) one can consider some extreme cases. For example, when the eavesdroppers in a coalition S spend the whole time slot duration θ_c for information exchange when eavesdropping on a user i, i.e., $\theta_{S,i} = 1$, then user i would have already transmitted all of its data without any tapping and in this case, cooperation is not beneficial for attacking i (although it may be beneficial for eavesdropping on another user $j \neq i$ in another time slot). On the other hand, if $\theta_{S,i} = 0$, then coalition S spends no time for information exchange, and, hence, the attack on user i is most efficient as the coalition S is able to perform receive beamforming on user i during the whole slot duration θ_c.

Having laid out the key components of the proposed eavesdroppers cooperation protocol, the rest of the paper is dedicated to investigate how a network of eavesdroppers can, in a distributed manner, perform this cooperation and form coalitions such as in Fig. 1 taking into account the various performance metrics previously described.

3. EAVESDROPPERS COOPERATION AS A COALITION FORMATION GAME

For mathematically modeling the eavesdroppers cooperation problem, we refer to coalitional game theory [18, 19] which provides a set of analytical tools suitable for modeling problems such as the one proposed in Section 2. In fact, the introduced eavesdroppers cooperation problem can be modeled as a coalitional game with a non-transferable utility which is defined as follows [18, Chap. 9]:

Definition 1. *A coalitional game with non-transferable utility is defined by a pair $(\mathcal{K}, V)$ where $\mathcal{K}$ is the set of players and V is a mapping such that for every coalition $S \subseteq \mathcal{K}$, $V(S)$ is a closed convex subset of $\mathbb{R}^{|S|}$ that contains the payoff vectors that players in S can achieve.*

In other words, a coalitional game has a non-transferable utility whenever the total utility achieved by any coalition S cannot be arbitrarily distributed among the members of S, hence, there is a need for a set of payoff vectors, i.e., the mapping V to describe the utilities achieved by the players in a coalition S. In the eavesdroppers cooperation model, the set of eavesdroppers $\mathcal{K}$ is the set of players in the coalitional game. In addition, given a coalition S and denoting by $\phi_k(S)$ the payoff of eavesdropper $k \in S$ achieved during

an eavesdropping cycle, we highlight the following property

Property 1. *The proposed cooperative eavesdropping game has a non-transferable utility where the payoff $\phi_k(S)$ received by any eavesdropper $k \in S$ during one eavesdropping cycle, i.e., the overall secrecy capacity reduction caused during one cycle by eavesdropper k when acting as part of S, is equal to the overall secrecy capacity reduction $u(S)$ achieved by the coalition S as given by (9).*

PROOF. Over an eavesdropping cycle, the presence of any coalition of eavesdroppers $S \subseteq \mathcal{K}$ implies that the maximum total secrecy capacity that the users in $\mathcal{N}$ can achieve is given by $u(S)$ in (9) which also represents the utility achieved by S. Clearly, this damage is a result of the contribution of every member of S. Consequently, one can see that the overall reduction in secrecy capacity that any eavesdropper $k \in S$ incurs on the users in $\mathcal{N}$ is given by the reduction that the coalition S induced on these users. Hence, $\phi_k(S) = u(S),\ \forall k \in S$. Consequently, this structure of the game implies that the value $u(S)$ of any coalition S as given by (9) cannot be distributed in an arbitrary manner between the members, since $\phi_k(S) = u(S)$ and thus the game has a non-transferable utility. □

Given Property 1, the mapping V for the eavesdroppers coalitional game can be defined as follows:

$$V(S) = \{\boldsymbol{\phi}(S) \in \mathbb{R}^{|S|} |\ \ \phi_k(S) = -u(S),\ \forall k \in S\}, \quad (10)$$

where $\boldsymbol{\phi}(S)$ is a vector of payoffs achieved during one eavesdropping cycle by the eavesdroppers when acting in coalition S, $u(S)$ is the overall secrecy capacity reduction incurred on the users in $\mathcal{N}$ as given by (9), and the *minus sign* is inserted in front of $u(S)$ in the payoff $\phi_k(S)$ for convenience to turn the game into a maximization problem (the objective of the eavesdroppers is initially to minimize $u(S)$). Clearly, the set $V(S)$ in the proposed game is a singleton set since a coalition S can only achieve a single utility value as dictated by (9). Consequently, this set is closed and convex, and the eavesdroppers cooperation problem is cast into a $(\mathcal{K}, V)$ coalitional game with non-transferable utility where the eavesdroppers aim to maximize their payoffs, hence, minimize the overall secrecy capacity achieved by the users (achieve maximum damage on the users) by forming coalitions.

Moreover, as explained in the previous section, the damage achieved by any coalition as per (9) takes into account a cost for cooperation. Consequently, given the cost of information exchange, we remark the following for the eavesdroppers cooperation coalitional game.

Property 2. *For the proposed $(\mathcal{K}, V)$ coalitional game, the grand coalition of all the users* seldom *forms due to the presence of a cost for cooperation. Hence, independent disjoint coalitions will appear in the network.*

PROOF. Consider a number of eavesdroppers positioned at different locations within the network. While cooperation improves the eavesdropping performance as per (4) and (9), this improvement is limited by the cost for cooperation given in (8). For instance, by closely investigating the cost for cooperation one can easily see that the cost grows as: (i)- The number of eavesdroppers in the coalition increase as seen in (8), and (ii)- As the channel (distance) between the eavesdroppers in the coalition, as well as the channel (distance) between the eavesdroppers and the users varies as seen through (5) and (7). As a simple example, by considering a network of two eavesdroppers separated by a very large distance, the time required for information exchange as per (8) can be close to 1, hence yielding no benefit for cooperation as per (9). Therefore, due to the various cooperation costs, the grand coalition of all users will *seldom* form (it only forms only in very favorable conditions which can be quite unrealistic in a large scale wireless network) and hence, the network structure consists of disjoint independent coalitions. □

As a result of Property 2, the proposed eavesdroppers cooperation game is classified as a *coalition formation game* due to the presence of cooperation costs and the fact that the grand coalition is not always the optimal solution [19, Sec. IV]. Consequently, solutions for canonical coalitional games such as the core may not be applicable. In fact, for the core of any coalitional game to exist as a solution concept, the game must ensure that the grand coalition of all players will form, and in addition, due to the non-transferable nature of the game, the mapping V must verify certain conditions [18, Chap. 9], [19]. However, as seen in Fig. 1 and corroborated by Property 2, the cost for coalition formation will generally forbid the formation of the grand coalition. Instead, a network composed of independent and disjoint coalitions will form as a result of the cooperative beamforming performed among the eavesdroppers. Therefore, the proposed game is a coalition formation game and the objective is to derive a distributed algorithm that will lead to coalitional structures such as the one shown in Fig. 1.

4. DISTRIBUTED EAVESDROPPERS COALITION FORMATION ALGORITHM

4.1 Coalition Formation Algorithm

Coalition formation games have been a topic of high interest in game theory [20, 21] and have recently also attracted attention in wireless and communication networks [19]. The goal is to find algorithms for characterizing the coalitional structures that form in a network where the grand coalition is not optimal. By using game theoretical concepts from coalition formation games, we introduce a distributed coalition formation algorithm for the proposed $(\mathcal{K}, V)$ eavesdroppers cooperation game. First, we require the following definitions [21]:

Definition 2. *A* collection *of coalitions, denoted by $\mathcal{S}$, is defined as the set $\mathcal{S} = \{S_1, \ldots, S_l\}$ of mutually disjoint coalitions $S_i \subset \mathcal{K}$. In other words, a collection is any arbitrary group of disjoint coalitions S_i of $\mathcal{K}$ not necessarily spanning all players of $\mathcal{K}$. If the collection spans* all *the players of $\mathcal{K}$; that is $\bigcup_{j=1}^{l} S_j = \mathcal{K}$, the collection is a* partition *of $\mathcal{K}$.*

Definition 3. *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 $\mathcal{A} \subseteq \mathcal{K}$ (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 $\mathcal{A}$.*

Several well known preference relations can be used in various scenarios [19, 21]. These orders can be divided into two categories: Coalition value orders and individual value orders. Coalition value orders compare two collections (or partitions) using the value function of the coalitions inside

these collections (suitable for games with transferable utilities) while individual value orders perform the comparison using the individual payoffs of every player. For the individual orders, two collections $\mathcal{R}$ and $\mathcal{S}$ are seen as two vectors of individual payoffs of the same length (corresponding to the total number of players) where each element of these payoff vectors corresponds to the utility received by the players in each coalition $R_i \in \mathcal{R}$ and $S_i \in \mathcal{S}$. In this context, individual value orders are quite suitable for non-transferable utility games such as the proposed game. Hence, we define the following individual order that can be used in the eavesdroppers cooperation game:

Definition 4. *Consider two collections* $\mathcal{R} = \{R_1, \ldots, R_l\}$ *and* $\mathcal{S} = \{S_1, \ldots, S_m\}$ *that are partitions of the same subset* $\mathcal{A} \subseteq \mathcal{K}$ *(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*

$$\mathcal{R} \rhd \mathcal{S} \Longleftrightarrow \{\Phi_j(\mathcal{R}) \geq \Phi_j(\mathcal{S}) \ \forall \ j \in \mathcal{R}, \mathcal{S}\}, \qquad (11)$$

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. For performing the coalition formation process among the eavesdroppers, we construct an algorithm based on two simples operations, so called "merge" and "split" rules, borrowed from coalition formation games [21] and defined as follows:

Definition 5. ***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 6. ***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,* $\{\bigcup_{j=1}^{l} S_j\} \rightarrow \{S_1, \ldots, S_l\}$*.*

By utilizing the merge rule, a number of coalitions can cooperate and form a larger coalition if this merge yields a preferred collection based on the Pareto order. This implies that a group of players can agree to form a larger coalition, if at least one of the players improves its payoff without decreasing the utilities of any of the other players. 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 players agree to sign a merge agreement, this agreement can only be broken if all the players approve. This is a family of coalition formation games known as coalition formation games with partially reversible agreements [20]. For the $(\mathcal{K}, V)$ eavesdroppers cooperation coalition formation game, the merge and split rules are suitable for forming the eavesdroppers coalitions due to numerous reasons. First, every merge or split decision can be taken individually, in a distributed manner by the eavesdroppers (or coalition of eavesdroppers). Moreover, as proven in [21] any algorithm built on iterations of merge and split will converge to a final partition, due to the nature of the preference relations used. Therefore, these rules can be used as building blocks in a coalition formation process for the eavesdroppers coalition formation game.

However, since the Pareto order defined in (11) relies on a comparison of the *instantaneous* payoffs (secrecy capacities) $\phi_k(S)$ (for any eavesdropper k in any coalition S) as given by (9), performing merge or split using this order requires a full knowledge of the channel gain including the fading amplitude as per (3). Due to the fact that the fading amplitude varies from one slot to the other, utilizing the Pareto order as in (11) may require performing merge and split every slot within every eavesdropping cycle, which can be a tedious task on the eavesdroppers. In addition, merging or splitting based on the instantaneous channel gains requires a continuous estimation of the instantaneous fading amplitude of the channel, which can again be quite a complex process.

For this purpose, and in order to avoid this complexity, we propose a *far sighted* approach to the merge and split rules whereby the eavesdroppers use the Pareto order in (11) based on their *long term payoff* $\bar{\phi}_k(S) = \bar{u}(S)$, which is defined as the payoff that the eavesdroppers receive during an eavesdropping cycle averaged over the fading amplitude realizations. As we consider a quasi-static channel model, one can easily see using (3) and (9) that the secrecy capacities, and payoffs $\bar{\phi}_k(S)$ averaged over the channel realizations will depend mainly on the path loss (distance) between the nodes (eavesdropper-eavesdropper, eavesdropper-user, or user-BS). Consequently, we propose that the eavesdroppers utilize a coalition formation algorithm based on *far sighted merge and split* rules that are constructed using the Pareto order in (11) applied to the long term average payoffs $\bar{\phi}_k(S)$ which are given by (9) when using the averaged channel gains. In this regard, any coalition formation algorithm based on the far sighted merge and split rules would no longer require a knowledge of the instantaneous fading amplitude as the decisions are based on long term utilities averaged over the fading amplitude.

Accordingly, for the eavesdroppers coalitional game, we construct a coalition formation algorithm based on far sighted merge-and-split operations and divided into three phases: neighbor discovery, adaptive far sighted coalition formation, and cooperative eavesdropping. In the neighbor discovery phase (Phase 1), each coalition (or eavesdropper) surveys its neighborhood for locating nearby eavesdroppers with whom cooperation is possible. At the end of this phase, each coalition would construct a list of its neighboring partners and proceeds to the next phase of the algorithm.

Following Phase 1, the adaptive far sighted coalition formation phase (Phase 2) debuts, whereby the coalitions (or individual eavesdroppers) interact with their neighbors for assessing whether to form new coalitions or whether to break their current coalition. For this purpose, an iteration of sequential far sighted merge-and-split rules occurs in the network, whereby each coalition decides to merge (or split) depending on the long term utility improvement that merging (or splitting) yields. This phase starts from an initial network partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ of $\mathcal{K}$. Subsequently, any random coalition (individual eavesdropper) can start with the merge process. For practicality purposes, consider that the coalition $T_i \in \mathcal{T}$ which has the highest long term utility in the initial partition $\mathcal{T}$ starts by attempting to merge with a nearby coalition. On one hand, if merging occurs, a new coalition of eavesdroppers $\tilde{T}_i$ is formed and, in its turn, $\tilde{T}_i$ will attempt to merge with nearby eavesdroppers (coalitions), if possible. On the other hand, if T_i is unable

to merge with the firstly discovered neighbor, it tries to find other coalitions that have a mutual benefit in merging. The search ends with a final merged coalition T_i^{final} composed of the eavesdroppers in T_i and one or several of coalitions in its vicinity ($T_i^{\text{final}} = T_i$, if no merge occurred). 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 $\mathcal{F}$ can next perform split operations, if any is possible. An iteration consisting of multiple successive merge-and-split operations is repeated until it converges. The convergence of an iteration of merge and split rules is guaranteed as shown in [21]. Note that the decisions to merge or split can be taken in a distributed way by the eavesdroppers without relying on any centralized entity.

In the cooperative eavesdropping phase (Phase 3), within every slot of an eavesdropping cycle, the coalitions exchange their information and begin their cooperative eavesdropping process, in a time slotted manner, one coalition per slot. Hence, in this phase, the eavesdroppers coalitions perform the actual receive beamforming, for efficiently tapping into the signal of the network's users within the corresponding slot. Each round of the proposed algorithm consists of these three phases, and is summarized in Table 1. For a stationary network, the last phase of the algorithm, i.e., the cooperative eavesdropping phase, is performed continuously over a large number of eavesdropping cycles. On the other hand, in a network where the eavesdroppers and/or the users are mobile, periodic runs of the first two phases of the proposed algorithms are performed which allows the eavesdroppers to autonomously self-organize and adapt the network's topology through appropriate merge-and-split decisions during Phase 2. This adaptation to environmental changes is performed in mobile networks periodically every M eavesdropping cycles. In general, the number of cycles M can be chosen arbitrarily but, for adapting to mobility, M must be smaller as mobility increases in order to allow adequate adaptation of the network.

The proposed algorithm in Table 1 can be implemented in a distributed manner. At the beginning of time, the eavesdroppers can detect the strength of the users' uplink signals, and, thus, estimate the location of these users. Note that, due to the far sighted merge-and-split rules considered, the eavesdroppers are not required to estimate the instantaneous fading amplitude of the channel (only an estimate of the users' locations is needed for evaluating the long term payoffs needed for coalition formation). Further, nearby coalitions (eavesdroppers) can be discovered in Phase 1 through techniques similar to those used in the ad hoc routing discovery process [22]. Once the neighbors are discovered and the users' locations are estimated, the coalitions can perform merge operations based in Phase 2. Moreover, each formed coalition can also internally decide to split if its members find a preferred split structure. During Phase 3, within every slot, the distributed eavesdroppers would exchange their information (channels, control, etc.) and then cooperate to perform receive beamforming using the cooperative protocol described in Section 2.2.

4.2 Partition Stability

The stability of any network partition resulting from the proposed algorithm in Table 1 can be investigated using the concept of a defection function [21].

Table 1: One round of the proposed eavesdroppers coalition formation algorithm

Initial State

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

Three phases in each round of the eavesdroppers coalition formation algorithm

Phase 1 - Neighbor Discovery:

a) Each coalition of eavesdroppers surveys its neighborhood for candidate partners.

Phase 2 - Adaptive Far Sighted Coalition Formation:

In this phase, coalition formation among the eavesdroppers using far sighted merge-and-split occurs.

repeat

a) $\mathcal{F} = \text{Merge}(\mathcal{T})$; coalitions in $\mathcal{T}$ decide to merge based on the algorithm described in Section 4.1.

b) $\mathcal{T} = \text{Split}(\mathcal{F})$; coalitions in $\mathcal{F}$ decide to split based on the Pareto order (using long term payoffs).

until merge-and-split converges.

Phase 3 - Cooperative Eavesdropping:

a) During every slot of an eavesdropping cycle, every coalition's eavesdroppers exchange their information and then perform receive beamforming for launching an efficient attack on the users (one user attacked per slot, Section 2.2)

b) For networks where the eavesdroppers and users are stationary, this phase is repeated continuously for a large number of eavesdropping cycles.

For networks where environmental changes such as mobility may occur, the above three phases are repeated periodically every M eavesdropping cycles.

Definition 7. *A* defection *function $\mathbb{D}$ is a function which associates with each partition $\mathcal{T}$ of $\mathcal{K}$ a group of collections in $\mathcal{K}$. A partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ of $\mathcal{K}$ is* $\mathbb{D}$-stable *if no group of players benefits from leaving $\mathcal{T}$ when the players who leave can only form the collections allowed by $\mathbb{D}$.*

For the eavesdroppers coalition formation game, two defection functions are of interest [19,21]. First, the $\mathbb{D}_{hp}$ function which associates with each partition $\mathcal{T}$ of $\mathcal{K}$ the group of all partitions of $\mathcal{K}$ that can form through merge or split and the $\mathbb{D}_c$ function which associates with each partition $\mathcal{T}$ of $\mathcal{K}$ the group of all collections in $\mathcal{K}$. The function $\mathbb{D}_c$ allows any group of players to leave the partition $\mathcal{T}$ of $\mathcal{K}$ through *any* operation and create an arbitrary *collection* in $\mathcal{K}$. 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 $\mathcal{T}$ benefits from leaving $\mathcal{T}$ through merge-and-split to form other partitions in $\mathcal{K}$; while a partition $\mathcal{T}$ is $\mathbb{D}_c$-stable, if no player in $\mathcal{T}$ is benefits from leaving $\mathcal{T}$ through *any* operation (not necessarily merge or split) to form other collections in $\mathcal{K}$.

Characterizing any type of $\mathbb{D}$-stability for a network partition depends on various properties of the coalitions that have formed. For instance, a partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ of $\mathcal{K}$ is $\mathbb{D}_{hp}$-stable if, for the partition $\mathcal{T}$, no coalition has an incentive to merge or split. An immediate result of this definition of $\mathbb{D}_{hp}$-stability is the following:

Lemma 1. *Every partition resulting from the coalition formation algorithm proposed for the eavesdroppers cooperation game in Table 1 is $\mathbb{D}_{hp}$-stable.*

In other words, a $\mathbb{D}_{hp}$-stable partition can be thought of as a state of equilibrium where no coalitions have an incentive to pursue coalition formation through merge or split.

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 (ii)- 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 $\mathcal{K}$, $\mathcal{T} \rhd \mathcal{T}'$. 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 when possible. However, the existence of a $\mathbb{D}_c$-stable partition is not always guaranteed [21]. The $\mathbb{D}_c$-stable partition $\mathcal{T} = \{T_1, \ldots, T_l\}$ of the whole space $\mathcal{K}$ exists if a partition of $\mathcal{K}$ that verifies the following two necessary and sufficient conditions exists [21]:

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 $G \subset \mathcal{K}$ 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 $\mathcal{K}$ can satisfy these conditions, then no $\mathbb{D}_c$-stable partition of $\mathcal{K}$ exists. Nevertheless, for the eavesdroppers cooperation game, we have:

Lemma 2. *For the proposed $(\mathcal{K}, v)$ eavesdroppers coalitional game, the proposed algorithm of Table 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. This result is a consequence of Lemma 1 and the fact that the $\mathbb{D}_c$-stable partition is a unique outcome of any merge-and-split iteration [21] which is the case with any partition resulting from our algorithm. □

For the proposed game, in order to satisfy the first condition for existence of the $\mathbb{D}_c$-stable partition, the eavesdroppers that are members of each coalition must verify the Pareto order through their long term payoff vectors as given by (9) and (10) averaged over the fading amplitude realizations. Similarly, for verifying the second condition of $\mathbb{D}_c$ stability, eavesdroppers belonging to all $\mathcal{T}$-incompatible coalitions in the network must also verify the Pareto order. Consequently, the existence of such a $\mathbb{D}_c$-stable partition is closely tied to the location of the eavesdroppers through the long term individual payoffs (long term secrecy capacities) as well as the locations of the eavesdroppers and users in the network. Hence, the existence of the $\mathbb{D}_c$-stable partition strongly depends on the positions of the users and the eavesdroppers, which, in a practical large scale ad hoc wireless network are generally random and may be time varying. Therefore, the existence of the $\mathbb{D}_c$-stable partition cannot be always guaranteed in the eavesdroppers cooperation game. However, despite this limitation, the proposed algorithm will always guarantee convergence to this optimal $\mathbb{D}_c$-stable partition when it exists as stated in Lemma 2. Whenever a $\mathbb{D}_c$-stable partition does not exist, the coalition structure resulting from the proposed algorithm will be a sub-optimal

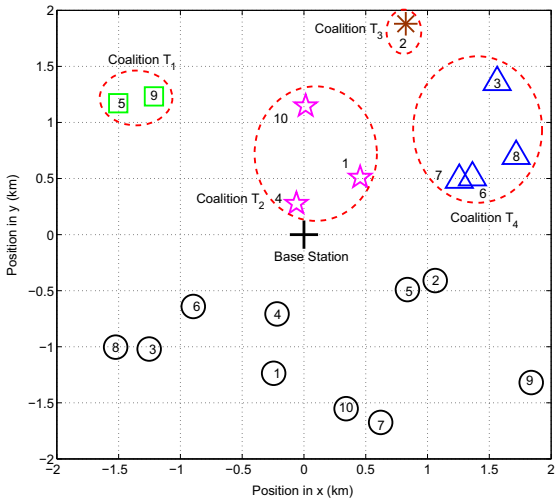

Figure 2: A snapshot of a coalitional structure resulting from our proposed coalition formation algorithm for a network with $K = 10$ eavesdroppers, and $N = 10$ users (circles).

$\mathbb{D}_{hp}$-stable partition (no coalition or individual user is able to merge or split any further).

5. SIMULATION RESULTS AND ANALYSIS

For simulations, a square network of 4 km × 4 km is set up with the BS located at the center, the eavesdroppers randomly placed at the upper 4×2 rectangle while the users are randomly deployed within the lower 4×2 rectangle. The simulation parameters used are as follows: First, the number of bits for information exchange is taken as $L = 128$ bits, the power constraint per eavesdropper/user is $\tilde{P} = 10$ mW, the noise level is -90 dBm, the channel propagation loss is set to $\alpha = 3$, and the bandwidth is $W = 100$ kHz. The Doppler frequency is set to 10 Hz (stationary/very low mobility) which yields a coherence time (slot duration) of 42.3 ms.

In Fig. 2, we show a snapshot of the network structure resulting from the proposed coalition formation algorithm for a randomly deployed network with $K = 10$ eavesdroppers, and $N = 10$ users. This figure shows how the eavesdroppers can cooperate and self-organize into 4 coalitions with the resulting network structure $\mathcal{T} = \{T_1, T_2, T_3, T_4\}$. For example, Eavesdropper 2 is unable to find any nearby partner to improve his payoff and hence decides to act alone. In contrast, Eavesdroppers 5 and 9 merge into a single coalition $T_1 = \{5, 9\}$ due to the fact that $V(\{5, 9\}) = \{\boldsymbol{\phi}(\{5, 9\}) = [-135 \cdot 10^4, \ -135 \cdot 10^4]\}$ which is a clear improvement on the non-cooperative utilities which were $\phi_5(\{5\}) = -177.32 \cdot 10^4$ and $\phi_9(\{9\}) = -174.44 \cdot 10^4$ (recall the minus sign in the utilities is inserted to turn the problem into a maximization problem). Similar results can also be seen for the formation of coalitions T_3 and T_4. In a nutshell, Fig. 2 shows how the eavesdroppers can self-organize into disjoint independent coalitions for performing cooperative eavesdropping through receive beamforming.

In Fig. 3 we show how the algorithm can handle mobility through appropriate coalition formation decisions. For this purpose, the network setup of Fig. 2 is considered while Eavesdropper 4 is moving horizontally for 0.35 km in the di-

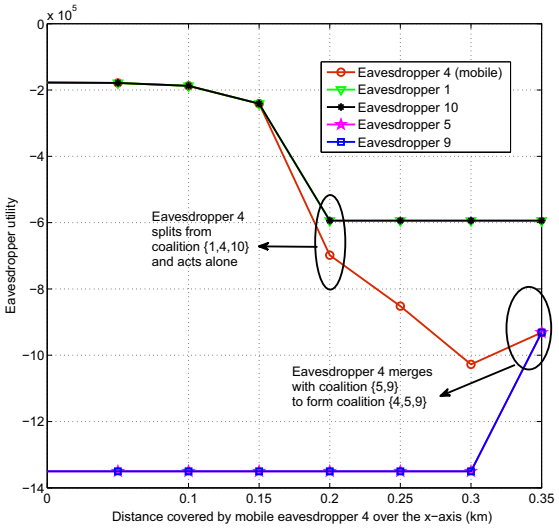

Figure 3: Self-adaptation of the network's topology to mobility as Eavesdropper 4 in Figure 2 moves horizontally on the negative x-axis.

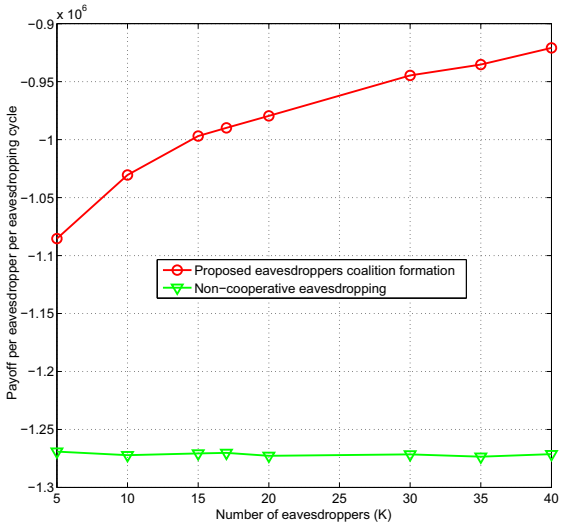

Figure 4: Payoff per eavesdropper per eavesdropping cycle (averaged over random locations of the eavesdroppers and users) achieved during $M = 600$ eavesdropping cycles (around 4 minutes) in a network with $N = 10$ users as the number of eavesdroppers K varies.

rection of the *negative* x-axis. As mobility starts, Eavesdropper 4 distances itself from its cooperating partners Eavesdroppers 1 and 10, hence its payoff (long term) drops. As Eavesdropper 4 moves 0.2 km, it splits from coalition $\{1, 4, 10\}$ and decides to act alone. This split is a result of the increase in the cost for information exchange due to Eavesdropper 4 distancing itself from its coalition partners 1 and 10 as well as the proximity of Eavesdropper 4 to the network's users (notably Users 4 and 6) which allows these users to tap into the information exchange phase, hence increasing the cost as per (7) and (8). In fact, when Eavesdropper 4 moves 0.2 km, the payoffs achieved by Eavesdroppers 1, 4, and 10 when acting within coalition $\{1, 4, 10\}$ are $V(\{1, 4, 10\}) = \{\phi(\{1, 4, 10\}) = [-98.75 \cdot 10^4,\ -98.75 \cdot 10^4,\ -98.75 \cdot 10^4]\}$ which are much smaller than the payoffs achieved by these eavesdroppers if they split into $\{1, 10\}$ and $\{4\}$ (once they split $V(\{1, 10\}) = \{\phi(\{1, 10\}) = [-59.41 \cdot 10^4,\ -59.41 \cdot 10^4,\ -59.41 \cdot 10^4]\}$ and $\phi_4\{4\} = -69.81 \cdot 10^4$). As Eavesdropper 4 moves 0.35 km, it merges with Eavesdroppers 5 and 9, forming a three-eavesdropper coalition $\{4, 5, 9\}$ while all three eavesdroppers improve their payoffs. Similar results can also be observed when all the eavesdroppers (or users) are moving, but are omitted due to space limitation.

In Fig. 4, for a network having $N = 10$ users, we show the payoff (secrecy capacity reduction) per eavesdropper achieved per eavesdropping cycle during a period of around 4.2 minutes, i.e., $M = 600$ eavesdropping cycles (each eavesdropping cycle consists of $N = 10$ slots) averaged over the random locations of the eavesdroppers and the users, as a function of the eavesdroppers network size K. The payoff shown is the actual payoff achieved by the eavesdroppers over this period given the instantaneous fading amplitudes of the channel following the coalition formation process. We compare the performance of the proposed eavesdroppers coalition formation algorithm to that of the non-cooperative case. For the cooperative case, the average eavesdropper's payoff increases with the number of eavesdroppers since the possibility of finding cooperating partners increases. Moreover, this increase is interpreted by the fact that, as more eavesdroppers are available, the efficiency of attacking several users also improves. In contrast, the non-cooperative approach presents an almost constant performance with different network sizes. Clearly, in Fig. 4, we can see that cooperation presents a significant advantage over the non-cooperative case in terms of average payoff per eavesdropper per eavesdropping cycle for all network sizes, and this advantage increases with K reaching up to 27.6% of improvement relative to the non-cooperative case at $K = 40$ eavesdroppers. In summary, Fig. 4 shows that by using the proposed coalition formation algorithm, the eavesdroppers can significantly improve the damage that they cause on the network users, i.e., reduce the secrecy capacities of these users.

In Fig. 5, for a network of $N = 10$ users, we evaluate the average and maximum coalition size (averaged over random locations of the eavesdroppers and users) resulting from the proposed coalition formation algorithm as the number of eavesdroppers K increases. In this figure, we can see that, as the number of eavesdroppers K increases, both the average and maximum coalition sizes increase. This is a direct result of the fact that, as K increases, the possibility of finding a cooperating partner becomes higher for all eavesdroppers. Further, by inspecting the average coalition size in Fig. 5, we remark that the coalitions resulting from the proposed algorithm are generally small, as the average coalition size does not exceed 4 for a network with $K = 40$ eavesdroppers. This result highlights the limitation that the cooperation costs impose on the network. Nonetheless, in some scenarios, large coalitions may emerge as seen through the average maximum coalition size shown in Fig. 5 which can reach around 8 for a network of $K = 40$ eavesdroppers. In a nutshell, Fig. 5 shows that, on the average, the network topology is composed of a large number of small coalitions rather than a small number of large coalitions, with the emergence of some large coalitions occasionally.

6. CONCLUSIONS

In this paper, we introduced a model for cooperation among the eavesdroppers in a wireless network and we studied the

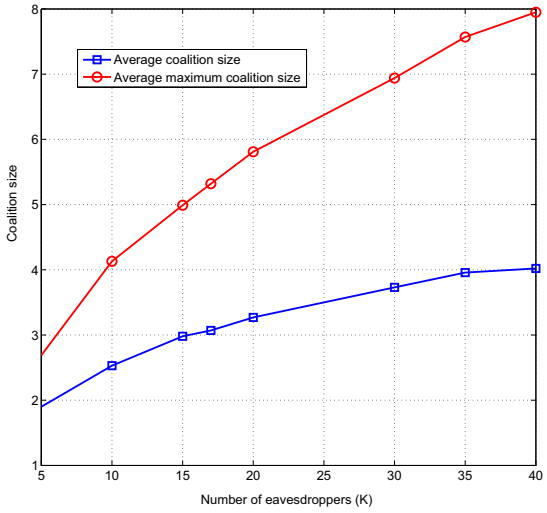

Figure 5: Average and average maximum (averaged over random locations of the eavesdroppers and users) coalition size achieved in a network with $N = 10$ users vs. the number of eavesdroppers K.

behavior, topology, and dynamics of the eavesdroppers' network through coalition formation games. In the introduced model, a number of single antenna eavesdroppers interact for forming cooperative coalitions that can utilize receive beamforming techniques to improve their attacks on the wireless users. We modeled the problem as a non-transferable coalitional game and classified it as a coalition formation game. Further, we proposed a coalition formation algorithm based on distributed rules of merge and split that allow the eavesdroppers to take autonomous decisions to form or break a coalition depending on their utility improvement. The utility of every coalition corresponds to the overall secrecy capacity reduction that the coalition can inflict on the network's users over the duration of an eavesdropping cycle. We studied the properties of the proposed coalition formation algorithm, we characterized the resulting network structures, we studied its stability, and analyzed the self-adaptation of the topology to environmental changes such as mobility. Simulation results show that the proposed algorithm allows the eavesdroppers to self-organize while improving the average payoff per eavesdropper up to 27.6% per eavesdropping cycle relative to the non-cooperative case. Finally, future work will consider cooperative defense mechanisms (against the eavesdroppers cooperation) for the users as well as discuss any possible equilibria, in terms of network partitions (at both the eavesdroppers and users sides), that can result when both the eavesdroppers and the users engage in coalition formation simultaneously.

7. REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[5] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4687–4698, Sep. 2008.

[6] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[7] P. Prada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[8] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. of 41st Conference on Information Sciences and Systems*, Baltimore, MD, USA, Mar. 2007.

[9] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. Allerton Conf. on Communication, Control, and Computing*, Monticello, IL, USA, Sep. 2008.

[10] A. Kashyap, T. Başar, and R. Srikant, "Correlated jamming on mimo gaussian fading channels," *IEEE Trans. InformatioN Theory*, vol. 50, pp. 2119–2123, Sep. 2004.

[11] T. S. Rappaport, *Wireless Communications: Principles and Practice, 2nd edition.* Prentice Hall, Dec. 2001.

[12] S. Mathur, L. Sankaranarayanan, and N. Mandayam, "Coalitional games in receiver cooperation for spectrum sharing," in *Proc. Conf. on Information Sciences and Systems*, New Jersey, NY, USA, Mar. 2006, pp. 949–954.

[13] H. Ochiai, P. Mitran, H. V. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks," *IEEE Trans. Signal Processing*, vol. 53, pp. 4110–4124, Nov. 2005.

[14] P. Viswanath, *Fundamentals of Wireless Communications.* Cambridge University Press, 2005.

[15] J. Litva and T. K. Y. Lo, *Digital Beamforming in Wireless Communications.* Artech House, 1996.

[16] L. C. Godara, *Smart Antennas.* CRC Press, 2004.

[17] A. Grant, "Performance analysis of transmit beamforming," *IEEE Trans. Commun.*, vol. 53, pp. 738–744, Apr. 2005.

[18] R. B. Myerson, *Game Theory, Analysis of Conflict.* Cambridge, MA, USA: Harvard University Press, Sep. 1991.

[19] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Başar, "Coalition game theory for communication networks: A tutorial," *IEEE Signal Processing Magazine, Special issue on Game Theory in Signal Processing and Communications*, to appear 2009.

[20] D. Ray, *A Game-Theoretic Perspective on Coalition Formation.* New York, USA: Oxford University Press, Jan. 2007.

[21] K. Apt and A. Witzel, "A generic approach to coalition formation," in *Proc. of the Int. Workshop on Computational Social Choice (COMSOC)*, Amsterdam, the Netherlands, Dec. 2006.

[22] C. S. R. Murthy and B. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols.* New Jersey, NY, USA: Prentice Hall, Jun. 2004.