Relay and Jammer Cooperation as a Coalitional Game in Secure Cooperative Wireless Networks

Rongqing Zhang*, Lingyang Song*, Zhu Han†, and Bingli Jiao*
*School of Electronics Engineering and Computer Science, Peking University, Beijing, China.
†Electrical and Computer Engineering Department, University of Houston, Houston, TX, USA.

***Abstract*—In this paper, we investigate cooperation of conventional relays and friendly jammers subject to secrecy constraints for cooperative networks. In order to obtain an optimized secrecy rate, the source selects several conventional relays and friendly jammers from the intermediate nodes to assist data transmission, and in return, it needs to make a payment. Each intermediate node here has two possible identities to choose, i.e., to be a conventional relay or a friendly jammer, which results in a different impact on the final utility of the intermediate node. After the intermediate nodes determine their identities, they seek to find optimal partners forming coalitions, which improves their chances to be selected by the source and thus to obtain the payoffs in the end. We formulate this cooperation as a coalitional game with transferable utility and study its properties. Furthermore, we define a Max-Pareto order for comparison of the coalition value, based on which we employ the merge-and-split rules. We also construct a distributed merge-and-split coalition formation algorithm for the defined coalition formation game. The simulation results verify the efficiency of the proposed coalition formation algorithm.**

I. Introduction

The basic idea of physical layer security is to exploit the physical characteristics of the wireless channel to provide secure communications. The security is quantified by the *secrecy capacity*, which is defined as the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers. This line of work was pioneered by Aaron Wyner, who introduced the wiretap channel and established fundamental results of creating perfectly secure communications without relying on private keys [1]. Follow-up work in [2] the secrecy capacity of Gaussian wiretap channel was studied, and in [3] Wyner's approach was extended to the transmission of confidential messages over broadcast channels. Cooperative jamming is considered as a promising approach to improve the secrecy capacity by interfering the eavesdropper with codewords independent of the source messages in a cooperative network. In [4], [5], several cooperative jamming schemes were investigated for different scenarios.

Cooperative game theory provides analytical tools to study the behavior of rational players when they cooperate. The main branch of cooperative games describes the formation of cooperating groups of players, referred to as coalitions, which can strengthen the players' positions in a game. Different classes of coalitional games for communication networks are introduced in [6]. Recently, researches on coalitional games used for distributed cooperation to improve the system performance have attracted lots of interest [7], [8].

SECURENETS 2011, May 16, Paris, France

DOI 10.4108/icst.valuetools.2011.246019

In this paper, we investigate conventional relay and friendly jammer cooperation for secure data transmission in a cooperative network. The source here can be regarded as a buyer who selects a group of several conventional relays and friendly jammers from the intermediate nodes in order to achieve an optimal secrecy rate, and in return it pays for the "service" offered by the selected nodes. Each intermediate node in the network has two identities to choose, i.e., to be a conventional relay or a friendly jammer, which is mainly determined according to its own channel conditions to the destination and the eavesdropper. After an intermediate node makes a choice of its identity, it starts to find some optimal partners to strengthen its opportunity to be selected by the source that may lead to a satisfactory payoff.

Specifically, we formulate this cooperation as a coalitional game with transferable utility. Some properties of the game are then studied, from which we find that the disjoint coalitions rather than the grand coalition will form in most cases, i.e., the coalitional game defined here can be classified as a coalition formation game. Furthermore, we define a Max-Pareto order for the value comparison between different coalitions, based on which we employ the merge-and-split rules. Then, we devise a distributed merge-and-split coalition formation algorithm of conventional relays and friendly jammers for the proposed game. Finally, the efficiency of the proposed coalition formation algorithm is verified by simulations. From the simulation results, we can see that the conventional relays and friendly jammers can self-organize into disjoint independent coalitions in a distributed manner and the algorithm achieves an efficient secrecy rate for data transmission.

The rest of this paper is organized as follows. In Section II, the system model of a cooperative network consisting of a couple of intermediate nodes is described. In Section III, we formulate this conventional relay and friendly jammer cooperation as a coalitional game with transferable utility and then study some properties of the proposed game. In Section IV, we construct a distributed coalition formation algorithm based on the merge-and-split rules. Simulation results are provided in Section V and the conclusions are drawn in Section VI.

II. System Model and Problem Formulation

As shown in Fig. 1, we consider a cooperative network consisting of one source node, one corresponding destination node, one malicious eavesdropper node, and N intermediate nodes, which are denoted by S, D, E, and T_i, $i = 1, 2, \ldots, N$,

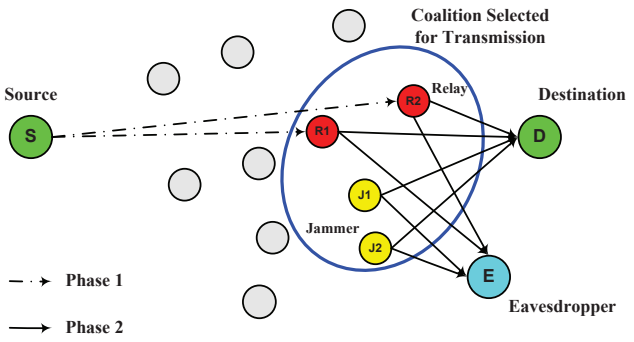

Fig. 1. System model for relay and jammer assisted secure cooperative network.

respectively. We denote by $\mathcal{T}$ the whole intermediate nodes set. All the nodes here are equipped with only a single omni-directional antenna and operate in a half-duplex way, i.e., each node cannot receive and transmit simultaneously. Then, the complete data transmission can be divided into two phases: 1) in the broadcasting phase, the source transmits its messages to the intermediate nodes, and the intermediate nodes who can successfully decode the signals from the source form a decoding node subset $\mathcal{T}_\mathcal{D} \subseteq \mathcal{T}$, and 2) in the cooperative relaying phase, several selected intermediate nodes transmit their signals towards both the destination and the eavesdropper with respect to secrecy constraints. Some of the selected nodes denoted by R_m, $m = 1, 2, \ldots, M$, operate as conventional relays, and forward the source messages to the destination. The other selected intermediate nodes denoted by J_k, $k = 1, 2, \ldots, K$, operate as friendly jammers who can transmit jamming signals to interfere the malicious eavesdropper in order to improve the secrecy rate of data transmission. We denote by $\mathcal{M}$ and $\mathcal{K}$ the set of indices $\{1, 2, \ldots, M\}$ and $\{1, 2, \ldots, K\}$, respectively.

Note that relay R_m, $m \in \mathcal{M}$, must belong to the decoding subset $\mathcal{T}_\mathcal{D}$, while friendly jammer J_k, $k \in \mathcal{K}$, can be any node of the node set $\mathcal{T}$ as it need not decode the source messages. Furthermore, we assume that there are no direct links between source and destination as well as between source and eavesdropper. As a result, the data transmission can only be performed through the intermediate nodes, and the eavesdropper cannot overhear the broadcast channels between source and intermediate nodes as the source-eavesdropper channel is blocked. This topology assumption follows the description in [10].

Suppose the selected relay R_m, $m \in \mathcal{M}$, transmits with power p_m^R. The channel gains from relay R_m to destination D and malicious eavesdropper E are $g_{R_m,D}$ and $g_{R_m,E}$, respectively. Friendly jammer J_k, $k \in \mathcal{K}$, transmits with power p_k^J to help improve the secrecy rate of data transmission from relay R_m to destination D. The channel gains from friendly jammer J_k to destination D and eavesdropper E are $g_{J_k,D}$ and $g_{J_k,E}$, respectively. Note that here the channel gain contains the path loss, as well as the Rayleigh fading coefficient with zero mean and unit variance. For simplicity, we assume that the fading coefficients are constant over one slot, and vary independently from one slot to another. The thermal noise at the destination and eavesdropper nodes satisfies independent Gaussian distribution with zero mean and same variance denoted by σ^2. The channel bandwidth is W.

First, with friendly jammers out of consideration, using maximal-ratio combining (MRC) at receiver, the channel capacity for data transmission from the selected relays to destination D, denoted by $C_{R\to D}(\{R_m\})$, $m = 1, 2, \ldots, M$, can be written as

$$C_{R\to D}(\{R_m\}) = \frac{W}{2}\log\left(1 + \frac{\sum\limits_m p_m^R g_{R_m,D}}{\sigma^2}\right). \quad (1)$$

Similarly, the channel capacity for data leakage from the selected relays to malicious eavesdropper E, denoted by $C_{R\to E}(\{R_m\})$, can be written as

$$C_{R\to E}(\{R_m\}) = \frac{W}{2}\log\left(1 + \frac{\sum\limits_m p_m^R g_{R_m,E}}{\sigma^2}\right). \quad (2)$$

The direct links $S \to D$ and $S \to E$ are not available in our assumptions, and thus, security of data transmission concerns only the cooperative relaying channels. Then, the secrecy rate for data transmission only via the selected relays can be defined as

$$\begin{aligned} C_s(\{R_m\}) &= \left(C_{R\to D}(\{R_m\}) - C_{R\to E}(\{R_m\})\right)^+ \\ &= \frac{W}{2}\left[\log\left(1 + \frac{\sum\limits_m p_m^R g_{R_m,D}}{\sigma^2}\right)\right. \\ &\quad \left. - \log\left(1 + \frac{\sum\limits_m p_m^R g_{R_m,E}}{\sigma^2}\right)\right]^+, \end{aligned} \quad (3)$$

where $(x)^+$ represents $\max\{x, 0\}$.

Taking friendly jammers into consideration, i.e., with the help of the friendly jammers transmitting jamming signals to interfere the malicious eavesdropper, the channel capacity for data transmission from the selected relays to destination D, denoted by $C_{R\to D}(\{R_m\}, \{J_k\})$, $m = 1, 2, \ldots, M$, $k = 1, 2, \ldots, K$, can be written as

$$C_{R\to D}(\{R_m\}, \{J_k\}) = \frac{W}{2}\log\left(1 + \frac{\sum\limits_m p_m^R g_{R_m,D}}{\sigma^2 + \sum\limits_k p_k^J g_{J_k,D}}\right). \quad (4)$$

Note that in our assumptions destination D is not able to mitigate the artificial interference from the friendly jammers, as the jamming signals are unknown to the destination.

Similarly, the channel capacity for data leakage from the selected relays to malicious eavesdropper E, denoted by $C_{R\to E}(\{R_m\}, \{J_k\})$, can be written as

$$C_{R\to E}(\{R_m\}, \{J_k\}) = \frac{W}{2}\log\left(1 + \frac{\sum\limits_m p_m^R g_{R_m,E}}{\sigma^2 + \sum\limits_k p_k^J g_{J_k,E}}\right). \quad (5)$$

Then, the secrecy rate for data transmission with the help of friendly jammers can be defined as

$$\begin{aligned} & C_s\left(\{R_m\},\{J_k\}\right) \\ = & \left(C_{R\to D}\left(\{R_m\},\{J_k\}\right)-C_{R\to E}\left(\{R_m\},\{J_k\}\right)\right)^+ \\ = & \frac{W}{2}\left[\log\left(1+\frac{\sum\limits_m p_m^R g_{R_m,D}}{\sigma^2+\sum\limits_k p_k^J g_{J_k,D}}\right)\right. \\ & \left.-\log\left(1+\frac{\sum\limits_m p_m^R g_{R_m,E}}{\sigma^2+\sum\limits_k p_k^J g_{J_k,E}}\right)\right]^+. \end{aligned} \tag{6}$$

III. Relay and Jammer Cooperation as a Coalitional Game

In this cooperative system, we consider the source as a buyer who wants to send its messages to the corresponding destination and to optimize the secrecy rate of data transmission with the help of conventional relays and friendly jammers, while in return it needs to pay for the "service". However, only one coalition consisting of several conventional relays and friendly jammers from the node set $\mathcal{T}$ can be selected by the source for secure data transmission. Thus, there exists competition among the intermediate nodes as each node wants to be selected and gets the payment from the source. The payment is determined by the amount of secrecy rate offered by the selected conventional relays and friendly jammers. Moreover, we assume that the source is sufficiently rich, i.e., the source cares much more about the secrecy rate of data transmission than the payment.

Then, in this section, we formulate the conventional relay and friendly jammer cooperation for secure data transmission described above as a coalitional game. In the proposed coalitional game, there involves a set of players, i.e., the intermediate nodes in the cooperative network, who seek to find optimal partners forming cooperative groups, in order to increase their counters in the selective transmission and to be selected by the source in the end maximizing their utilities.

A. Coalitional Game Definition

We define the intermediate nodes cooperation as a coalitional TU-game $(\mathcal{T}, v)$, where $\mathcal{T}$ denotes the set of players, i.e., the intermediate nodes $\{T_1, T_2, \ldots, T_N\}$, and $v(\mathcal{S})$ is the utility of a coalition $\mathcal{S}$, $\mathcal{S} \subseteq \mathcal{T}$. The value v of a coalition $\mathcal{S}$ can be given as

$$\begin{aligned} v(\mathcal{S}) = \frac{W}{2}\left[\log\left(1+\frac{\varepsilon_r\sum_{m=1}^{M_S} p_m^R g_{R_m,D}}{\sigma^2+\sum_{k=1}^{K_S} p_k^J g_{J_k,D}}\right)\right. \\ \left.-\log\left(1+\frac{\varepsilon_r\sum_{m=1}^{M_S} p_m^R g_{R_m,E}}{\sigma^2+\sum_{k=1}^{K_S} p_k^J g_{J_k,E}}\right)\right]^+, \end{aligned} \tag{7}$$

where ε_r is a switching factor that $\varepsilon_r = 1$ when there exists at least one conventional relay in $\mathcal{S}$ and $\varepsilon_r = 0$ when there is no conventional relay in $\mathcal{S}$. M_S and K_S represent the number of conventional relays and friendly jammers in the coalition, respectively, satisfying $M_S + K_S = |\mathcal{S}|$, where $|\mathcal{S}|$ denotes the total number of members in the coalition.

Each node in the node set $\mathcal{T}$ has two identities to choose, to be a conventional relay or to be a friendly jammer. To choose a proper identity is quite important for an intermediate node, for it has great effects on whether the intermediate node can find optimal partners to form a coalition and to be selected by the source in the end. The source will choose the coalition who can provide the highest secrecy rate for data transmission. Suppose that each intermediate node is selfish and rational, whose objective is to maximize its own utility. We denote by $\mathcal{N}$ the set of indices $\{1, 2, \ldots, N\}$. The channel gains from the intermediate node T_i to destination D and malicious eavesdropper E are $g_{T_i,D}$ and $g_{T_i,E}$, respectively, $i \in \mathcal{N}$.

During the cooperation course, each intermediate node will firstly choose its proper identity, i.e., to be a conventional relay or a friendly jammer, mainly according to its own channel conditions. Then, the intermediate nodes are divided into two groups, i.e., the relay group and the jammer group. We denote the relay group and the jammer group by $\mathcal{R} = \{R_1, R_2, \ldots, R_t\}$ and $\mathcal{J} = \{J_1, J_2, \ldots, J_l\}$, respectively, where $\mathcal{R} \cup \mathcal{J} = \mathcal{T}$.

Consider a coalition $\mathcal{S}$ with only one member T_i, $T_i \in \mathcal{T}$, either a conventional relay or a friendly jammer. Then, from the coalition value defined in (7), we can obtain the self-utility of T_i, i.e., the coalition value of $\mathcal{S} = \{T_i\}$, as

$$\begin{aligned} & U(T_i) \\ = & v\left(\mathcal{S}=\{T_i\}\right) \\ = & \begin{cases} \left[\log\left(1+\frac{p_{T_i}^R g_{T_i,D}}{\sigma^2}\right)-\log\left(1+\frac{p_{T_i}^R g_{T_i,E}}{\sigma^2}\right)\right]^+, & T_i\in\mathcal{R} \\ 0, & T_i\in\mathcal{J} \end{cases}. \end{aligned} \tag{8}$$

In addition, we define a payoff division rule of a coalition, which is to divide the extra utility equally among the members. Thus, the payoff utility of member T_i in a coalition $\mathcal{S}$ can be given as

$$\phi_i^v = \frac{1}{|\mathcal{S}|}\left(v(\mathcal{S}) - \sum_{T_j\in\mathcal{S}} U\left(T_j\right)\right) + U\left(T_i\right), \tag{9}$$

where $U(T_i)$ and $U(T_j)$ are the self-utility of intermediate node T_i and T_j defined in (8).

Theorem 1: For the intermediate node T_i, $i \in \mathcal{N}$, we have that if $g_{T_i,D} > g_{T_i,E}$ and $T_i \in \mathcal{T}_\mathcal{D}$, T_i will choose to be a conventional relay, otherwise, it will choose to be a friendly jammer.

Proof: First, we consider the intermediate nodes which cannot successfully decode the source messages during the broadcasting phase. If the intermediate node $T_i \notin \mathcal{T}_\mathcal{D}$, then the only choice for it is to be a friendly jammer as it does not satisfy the necessary condition of being a conventional relay.

Then, we consider the intermediate nodes which belong to the decoding subset $\mathcal{T}_\mathcal{D}$. For the case that $g_{T_i,D} > g_{T_i,E}$, if T_i chooses to be a conventional relay, from (8), we have that it can get a positive self-utility. If T_i chooses to be a friendly jammer, from (8), we have that the self-utility of it is zero, in addition, no one will want to cooperate with it for that with a positive jamming power it can only decrease the

secrecy rate achieved by a coalition due to (6). Therefore, the optimal choice of T_i under the channel condition that $g_{T_i,D} > g_{T_i,E}$ is to be a conventional relay. For the case that $g_{T_i,D} \leq g_{T_i,E}$, from (8), the self-utility will be zero either T_i chooses to be a conventional relay or a friendly jammer. However, if T_i chooses to be a friendly jammer, it may find some potential partners to form a stronger coalition and get a positive payoff utility from the formed coalition due to (9) for that it can increase the secrecy rate achieved by a coalition with a proper positive jamming power. Therefore, the optimal choice of T_i under the channel condition that $g_{T_i,D} \leq g_{T_i,E}$ is to be a friendly jammer. ■

B. Property of the Proposed Coalitional Game

Definition 1: A coalitional game $(\mathcal{T}, v)$ with transferable utility is said to be *superadditive* if for any two disjoint coalitions $\mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{T}$, $v(\mathcal{S}_1 \cup \mathcal{S}_2) \geq v(\mathcal{S}_1) + v(\mathcal{S}_2)$.

Property 1: The proposed coalitional game $(\mathcal{T}, v)$ is non-superadditive.

Proof: Consider two disjoint coalitions $\mathcal{S}_1 \subset \mathcal{T}$ and $\mathcal{S}_2 \subset \mathcal{T}$ in the network with their corresponding utilities $v(\mathcal{S}_1)$ and $v(\mathcal{S}_2)$ when they do not cooperate with each other. We assume that there is one node belongs to $\mathcal{R}$ in $\mathcal{S}_1$, which is denoted by R, while all the nodes belong to $\mathcal{J}$ in $\mathcal{S}_2$. Then, we have that $\varepsilon_r = 1$ in the coalition value $v(\mathcal{S}_1 \cup \mathcal{S}_2)$ and $v(\mathcal{S}_1)$, while $v(\mathcal{S}_2) = 0$ as $\varepsilon_r = 0$ for the value of coalition $\mathcal{S}_2$. From the expressions of (6) and (7), when $\varepsilon_r = 1$, in our assumptions we have that $v(\mathcal{S}) = (C_{R\to D}(R, \{J_k\}) - C_{R\to E}(R, \{J_k\}))^+$, where both $C_{R\to D}(R, \{J_k\})$ and $C_{R\to E}(R, \{J_k\})$ are decreasing and convex functions of $|\mathcal{S}| - 1$ which is the number of friendly jammers in the coalition $\mathcal{S}$ consisting of relay R and several friendly jammers. However, $C_{R\to E}(R, \{J_k\})$ decreases faster than $C_{R\to D}(R, \{J_k\})$ as the number of friendly jammers in $\mathcal{S}$ increases, due to the channel conditions that $g_{J_k,D} < g_{J_k,E}$, $\forall J_k \in \mathcal{J}$. Thus, $v(\mathcal{S})$ will increase in some region of $|\mathcal{S}| - 1$. But when $|\mathcal{S}| - 1$ further increases, both $C_{R\to D}(R, \{J_k\})$ and $C_{R\to E}(R, \{J_k\})$ approach zero, as a result, $v(\mathcal{S})$ will approach zero. From the above analysis, we can get that there exists an optimal number of friendly jammers i_{opt}, which can maximize the coalition value $v(\mathcal{S})$. Therefore, in the case that $||\mathcal{S}_1 \cup \mathcal{S}_2| - 1 - i_{opt}| > ||\mathcal{S}_1| - 1 - i_{opt}|$, $v(\mathcal{S}_1 \cup \mathcal{S}_2) < v(\mathcal{S}_1) + v(\mathcal{S}_2)$, which means that the proposed coalitional game is not superadditive. ■

Definition 2: Given the grand coalition $\mathcal{T}$ consisting of all the intermediate nodes, a payoff vector $\phi^v = (\phi_1^v, \phi_2^v, \ldots, \phi_N^v)$ for dividing the coalition value $v(\mathcal{T})$ is said to be *group rational* if $\sum_{i=1}^{N} \phi_i^v = v(\mathcal{T})$, and to be *individually rational* if each player can obtain a benefit no less than acting alone, i.e., $\phi_i^v \geq v(\{T_i\}), \forall i \in \mathcal{N}$. An *imputation* is a payoff vector satisfying the above two conditions.

Having defined an imputation, the core can be defined as

$$\mathcal{C}_{TU} = \left\{ \phi^v : \sum_{T_i \in \mathcal{T}} \phi_i^v = v(\mathcal{T}) \text{ and } \sum_{T_i \in \mathcal{S}} \phi_i^v \geq v(\mathcal{S}), \forall \mathcal{S} \subseteq \mathcal{T} \right\}. \tag{10}$$

In other words, the core is the set of imputations where the players have no incentive to reject the proposed payoff allocation, deviate from the grand coalition $\mathcal{T}$ and form a coalition $\mathcal{S}$ instead. A non-empty core means that the players have an incentive to form the grand coalition.

Property 2: The core of the proposed coalitional game $(\mathcal{T}, v)$ is not always non-empty.

Proof: For this property, we consider a special case that there is only a few conventional relays but a large size of friendly jammers in $\mathcal{T}$, then from the proof to Property 1 we can get that the grand coalition value $v(\mathcal{T})$ approaches zero due to the high interference of friendly jammers, which will lead to no group rational imputation. Therefore, at least under this case the core of the proposed coalitional game is not non-empty. ■

Briefly, as a result of the non-superadditivity as well as the possible core's emptiness of the proposed game, the grand coalition of all the intermediate nodes will seldom form. Instead, several intermediate nodes will deviate from the grand coalition and form independent disjoint coalitions. Hence, in the next section, we will devise an algorithm for coalition formation that can characterize these disjoint coalitions.

IV. Coalition Formation Algorithm

From the above analysis, we find that disjoint coalitions rather than the grand coalition will form among the cooperative intermediate nodes in most cases. Thus, the proposed game can be classified as a *coalition formation game* [6]. In this section, using the game theoretical techniques from coalition formation games, we devise a distributed coalition formation algorithm.

A. Coalition Formation Concepts

For constructing a coalition formation process suitable to the proposed game, we require several definitions as follows.

Definition 3: A *collection* of coalitions, denoted by $\mathcal{P}$, is defined as a set $\mathcal{P} = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_p\}$ of mutually disjoint coalitions $\mathcal{S}_i \subset \mathcal{T}$. In other words, a collection is any arbitrary group of disjoint coalitions $\mathcal{S}_i$ of $\mathcal{T}$ not necessarily spanning all the players of $\mathcal{T}$. If a collection $\mathcal{P}$ spans all the players of $\mathcal{T}$, i.e., $\bigcup_{i=1}^{p} \mathcal{S}_i = \mathcal{T}$, then the collection is recognized as a *partition* of $\mathcal{T}$.

Definition 4: Consider two collections $\mathcal{P} = \{\mathcal{S}_1, \ldots, \mathcal{S}_p\}$ and $\mathcal{L} = \{\mathcal{S}_1^*, \ldots, \mathcal{S}_l^*\}$ which are partitions of the same subset $\mathcal{A} \subseteq \mathcal{T}$ (i.e., same players in $\mathcal{P}$ and $\mathcal{L}$). Then, a *comparison relation* $\rhd$ is defined as that $\mathcal{P} \rhd \mathcal{L}$ implies the way $\mathcal{P}$ partitions $\mathcal{A}$ is preferred to the way $\mathcal{L}$ partitions $\mathcal{A}$.

Various well known orders can be used as comparison relations [11]. There are two main categories of these orders, which are coalition value orders and individual value orders. Coalition value orders compare two collections using the value of the coalitions in these collections such as the utilitarian order in which $\mathcal{P} \rhd \mathcal{L}$ implies $\sum_{i=1}^{p} v(\mathcal{S}_i) > \sum_{i=1}^{l} v(\mathcal{S}_i^*)$. Individual value orders perform the comparison using the individual payoffs of each player such as the Pareto order. Given that two collections $\mathcal{P}$ and $\mathcal{L}$ have same players and

the payoffs of a player T_j in $\mathcal{P}$ and $\mathcal{L}$ are denoted by $\phi_j^v(\mathcal{P})$ and $\phi_j^v(\mathcal{L})$, respectively. The Pareto order can be written as

$$\mathcal{P} \rhd \mathcal{L} \Leftrightarrow \left\{\phi_j^v(\mathcal{P}) \geq \phi_j^v(\mathcal{L}),\ \forall T_j \in \mathcal{P}, \mathcal{L}\right\}, \qquad (11)$$

with at least one strict inequality ($>$) for a player T_k. The Pareto order implies a collection $\mathcal{P}$ is preferred to $\mathcal{L}$, if at least one player is able to improve its payoff when the coalition structure changes from $\mathcal{P}$ to $\mathcal{L}$ without decreasing other players' payoffs.

In this cooperative network, different coalitions of conventional relays and friendly jammers not only have chances for cooperation, but also suffer competition from each other as there is only one coalition can be selected by the source and gain the payoff in the end. Two disjoint coalitions are preferred to cooperate with each other if they can form a stronger one instead, as the players of them have more chance to win the payoffs from the source. Here, we concern more about the coalition who has the highest value and whether the players in it can always benefit from a positive payoff. Then, based on the Pareto order described in (11), we define a new comparison relation with respect to our system as follows.

Definition 5: Consider two collections $\mathcal{P} = \{\mathcal{S}_1, \ldots, \mathcal{S}_p\}$ and $\mathcal{L} = \{\mathcal{S}_1^*, \ldots, \mathcal{S}_l^*\}$ with same players in them. Then, the *Max-Pareto order* is defined as

$$\begin{aligned}\mathcal{P} \succ \mathcal{L} \Leftrightarrow\ & \{\max\{v(\mathcal{S}_1), \ldots, v(\mathcal{S}_p)\} \geq \max\{v(\mathcal{S}_1^*), \ldots, v(\mathcal{S}_l^*)\}, \\ & \text{and } \phi_j^v(\mathcal{P}) \geq \phi_j^v(\mathcal{L}),\ \forall T_j \in \mathcal{P}, \mathcal{L}\}, \end{aligned} \qquad (12)$$

with at least one strict inequality ($>$) for a player T_j in the individual payoff comparison.

B. Merge-and-Split Coalition Formation Algorithm

Using the coalition formation concepts in the previous subsection, we construct a distributed coalition formation algorithm for self-organization in the cooperative network based on two simple rules denoted as "merge" and "split" which permit to modify a partition of $\mathcal{T}$ [11].

- **Merge Rule:** Merge any set of coalitions $\{\mathcal{S}_1, \ldots, \mathcal{S}_l\}$ whenever the merged form is preferred by the players, i.e., where $\left\{\bigcup_{j=1}^{l} \mathcal{S}_j\right\} \succ \{\mathcal{S}_1, \ldots, \mathcal{S}_l\}$, then, $\{\mathcal{S}_1, \ldots, \mathcal{S}_l\} \longrightarrow \left\{\bigcup_{j=1}^{l} \mathcal{S}_j\right\}$.
- **Split Rule:** Split any coalition $\left\{\bigcup_{j=1}^{l} \mathcal{S}_j\right\}$ whenever a split form is preferred by the players, i.e., where $\{\mathcal{S}_1, \ldots, \mathcal{S}_l\} \succ \left\{\bigcup_{j=1}^{l} \mathcal{S}_j\right\}$, then, $\left\{\bigcup_{j=1}^{l} \mathcal{S}_j\right\} \longrightarrow \{\mathcal{S}_1, \ldots, \mathcal{S}_l\}$.

According to the above rules, multiple coalitions can merge into a larger coalition if merging yields a preferred partition based on the Max-Pareto order. This implies that a group of players can agree to form a larger coalition, if the merged coalition has no less value than any of the disjoint coalitions and at least one of the players can improve its payoff without decreasing the utilities of any other player. Similarly, an existing coalition can decide to split to smaller coalitions if splitting yields a preferred partition based on the Max-Pareto order.

As shown in Table I, we construct a distributed coalition formation algorithm based on the merge-and-split rules. The three phases of the coalition formation algorithm are repeated periodically during the network operation, allowing a topology that is adaptive to environmental changes such as mobility. During the adaptive coalition formation phase, $\mathcal{T}_t$ denotes the partition of the intermediate nodes set at clock t. The merging operation **Merge**$(\mathcal{T}_t)$ spans all the current coalitions in $\mathcal{T}_t$ orderly, resulting in a final partition $\mathcal{P}_t$ at clock t. Following the merge process, the coalitions in the resulting partition $\mathcal{P}_t$ are next subject to the splitting operation **Split**$(\mathcal{P}_t)$, if any is necessary. The process will be repeated until there is no need for any merging or splitting in the current partition. Note that the merge or split decisions can be taken in a distributed manner by each individual coalition without relying on any centralized entity.

TABLE I
THE PROPOSED DISTRIBUTED MERGE-AND-SPLIT COALITION FORMATION ALGORITHM

∗ **Initial State:**
The set of intermediate nodes is partitioned by $\mathcal{T}_0 = \{T_1, T_2, \ldots, T_N\}$ at the beginning with non-cooperation.

∗ **Coalition Formation Algorithm:**
⋆ *Phase 1 - Identity Choice:*
The source transmits its data to the intermediate nodes. Each intermediate node chooses its optimal identity (to be a conventional relay or a friendly jammer) based on its channel conditions to the destination and the eavesdropper.
For an intermediate node T_i, if $g_{T_i,D} > g_{T_i,E}$, then it will choose to be a conventional relay. Else, it will choose to be a friendly jammer. The intermediate node who cannot decode the source messages correctly has no choice but to be a friendly jammer.
⋆ *Phase 2 - Adaptive Coalition Formation:*
Each intermediate node with an identity can be regarded as a disjoint independent coalition, then coalition formation using merge-and-split rules occurs:
– Clock index $t = 0$.
– **Repeat**
(a) $\mathcal{P}_t =$ **Merge**$(\mathcal{T}_t)$: coalitions in $\mathcal{T}_t$ decide to merge based on the merge rules.
(b) $\mathcal{L}_t =$ **Split**$(\mathcal{P}_t)$: coalitions in $\mathcal{P}_t$ decide to split based on the split rules.
(c) Update clock index $t = t + 1$.
(d) Value assignment $\mathcal{T}_t = \mathcal{L}_t$.
Until merge-and-split terminates.
– Each coalition reports the secrecy rate of data transmission that it can achieve, i.e, the coalition value as we defined in (7), to the source.
⋆ *Phase 3 - Secure Transmission:*
The source chooses the coalition who can provide the highest secrecy rate for secure data transmission and pays for it.

V. Simulation Results

To validate the performances, we conduct the following simulations. For simplicity and without loss of generality, we consider a cooperative network with a couple of intermediate nodes in a 0.5×0.5 square area whose center is $(0, 0)$. Source S, destination D, and eavesdropper E are located at $(-2, 0)$, $(2, 0)$, and $(2, -1)$, respectively. The other simulation parameters are set up as follows: The jamming power of a friendly jammer is $p^J = 0.1p^R$, where p^R is the transmitting power of a conventional relay; the transmission bandwidth is $W = 1$; the noise variance is $\sigma^2 = 0.01$; Rayleigh fading channel is assumed, where the channel gain consists of both the path loss and the Rayleigh fading coefficient; the path loss factor is 2.

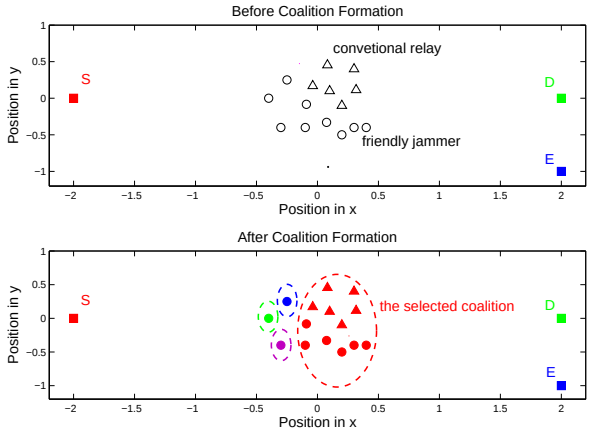

Fig. 2. Network scenarios before and after coalition formation.

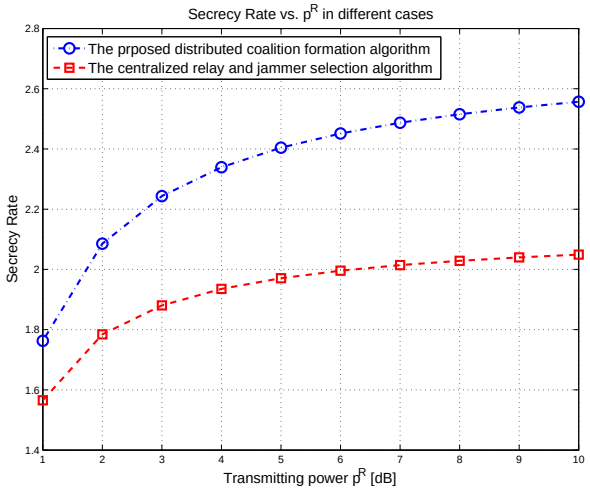

Fig. 3. Secrecy rate for data transmission in different cases.

In Fig. 2, we show the network scenarios before and after coalition formation based on our proposed merge-and-split algorithm. We can see that before coalition formation each intermediate node chooses its optimal identity (to be a conventional relay or a friendly jammer, in the figure △ represents conventional relay and ○ represents friendly jammer) according to its own channel conditions to the destination and the eavesdropper. Then, the conventional relays and friendly jammers start to find optimal partners in order to improve the chance to be selected by the source, using the merge-and-split rules to help them make decisions. After the coalition formation process, several disjoint independent coalitions are formed. The coalition with the highest value will be selected by the source for secure data transmission and obtain the payoff it deserves. Overall, this figure shows how the distributed conventional relays and friendly jammers can self-organize into disjoint independent coalitions based on the proposed merge-and-split algorithm. In addition, from the figure, we can find that all the conventional relays will always join in one coalition in the end.

In Fig. 3, we show the performance in terms of the final secrecy rate for data transmission as a function of the transmitting power p^R in two different cases. Here, the centralized relay and jammer selection algorithm is the one proposed as optimal selection with jamming (OSJ) scheme in [10]. The comparison between the two performance results implies the efficiency of our proposed distributed coalition formation algorithm with respect to secure data transmission in a cooperative network.

VI. Conclusions

In this paper, we have investigated cooperation of conventional relays and friendly jammers for secure data transmission in a cooperative network. We formulated this cooperation as a coalition formation game with transferable utility and studied some properties of it. Then, we devised a distributed coalition formation algorithm based on the merge-and-split rules. From the simulation results, we can see the efficiency of the proposed merge-and-split coalition formation algorithm.

Acknowledgment

This work was partially supported by the US NSF CNS-0953377, CNS-0905556, and CNS-0910461, and also by the National Nature Science Foundation of China under grant number 60972009 and 61061130561, as well as the National Science and Technology Major Project of China under grant number 2009ZX03003-011, 2010ZX03003-003, and 2011ZX03005-002.

References

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

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[5] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[6] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Basar, "Coalitional game theory for communication networks," *IEEE Signal Processing Magazine*, vol. 26, no. 9, pp. 77–97, Sep. 2009.

[7] W. Saad, Z. Han, M. Debbah, and A. Hjørungnes, "A distributed coalition formation framework for fair user cooperation in wireless network," *IEEE Transactions on Wireless Communications*, vol. 8, no. 9, pp. 4580–4593, Sep. 2009.

[8] W. Saad, Z. Han, M. Debbah, and A. Hjørungnes, "Physical layer security: Coalitional games for distributed cooperation," in *Proceedings of International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, Jun. 2009.

[9] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Transactions on Wireless Communications*, vol. 6, no. 9, pp. 3450–3460, Sep. 2007.

[10] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

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