Enhancing Wireless Security via Optimal Cooperative Jamming

Yunus Sarikaya, Ozgur Gurbuz

Abstract

In this work, we analyze the secrecy rate in a cooperative network, where a source node is assisted by relay nodes via cooperative jamming for delivering a secret message to the destination in the presence of an eavesdropper node. We consider the availability of both full and partial channel state information (CSI), and we take into account average power limitation at the relays as we formulate the rate maximization problem as a primal-dual problem. We derive the closed form solution for the full CSI case, and we show that the optimal solution allows the transmission of only one relay. For the partial CSI case, we define the concept of secrecy outage, where some of packets are intercepted by the eavesdropper, and we derive the secrecy outage probability and throughput in terms of average channel statistics. Due to the high nonlinearity of the secrecy throughput term, we propose a gradient update algorithm for obtaining the optimal power solutions for the partial CSI case. Our simulations demonstrate the gains of cooperative jamming over direct transmission for both full and partial CSI cases, where it is shown that the secrecy rate of the direct transmission is increased significantly, by $\%20-\%80$, when cooperative jamming is employed with our optimal power assignment algorithm.

Index Terms

Physical layer security, cooperative jamming, dual algorithm, gradient update algorithm.

I. Introduction

Confidentiality is a fundamental requirement for communication over wireless networks, since the broadcast nature of the wireless medium gives rise to a number of security issues. Basically, any node within the range of a transmitter node can eavesdrop the channel and it can extract the transmission over the so-called eavesdropper channel. Existing cryptography techniques, which mainly depend on secret keys address the security needs of wireless networks; however they fail to provide unconditional security. Moreover, the distribution and maintenance of secret keys are still open issues for large scale wireless networks. Fortunately, in the seminal paper of Wyner [1], it is shown that, when the main channel is a degraded version of the eavesdropper channel, a source node can send secret messages to a destination node with non-zero rate via Wyner secrecy encoding, while keeping the eavesdropper completely ignorant of the messages. The rate at which the destination node can decode the message, is defined as the secrecy rate. In [2], the "secrecy rate" region of broadcast channels is obtained. Recently, the concept of physical layer security introduced by Wyner is revisited in [3], where the wireless channel characteristics, such as fading and noise are exploited for improving the security of the main channel without degrading the eavesdropper channel.

The issue with physical layer security is that the secrecy rate is affected by the quality of the source-destination and the source-eavesdropper channels. Specifically, the secrecy rate can be very small, as low as zero in secrecy outage, when the eavesdropper has better channel conditions than the source. A possible solution is to utilize multiple-input multiple-output (MIMO) systems, where by using multiple antennas, the source-eavesdropper channel can be disrupted, and the information obtained by the eavesdropper can be reduced [4]. Cooperative communication

Y.Sarikaya (email: sarikaya@su.sabanciuniv.edu) and O. Gurbuz (email: ogurbuz@sabanciuniv.edu) are with the Faculty of Engineering and Natural Sciences, Sabanci University, 34956 Istanbul, Turkey.

can also increase the secrecy rate by exploiting the relay channels via cooperative jamming, where a relay creates interference at the eavesdropper by transmitting a jamming signal. The jamming signal power should be high enough to disturb the received signal at the eavesdropper; however allocating too much power on the jamming signal can also degrade the signal quality at the destination. Thus, it is essential to assign the jamming power levels optimally, so that the secrecy rate can be maximized. Among the existing works, [5] studies the use of decode-and-forward (DF) relays with multiple eavesdroppers, [6] analyzes both DF and amplify-and-forward (AF) cooperative schemes with a constraint on total power at the relays, and [8] considers both DF and AF cooperative schemes with individual power constraints at each relay. In a recent work, [7], the cooperative jamming (CJ) power allocation problem is solved with convex optimization and a one-dimensional search algorithm. The solutions proposed in the existing works are not only sub-optimal, since they are obtained by nulling out the jamming signal at the destination, but also they are obtained considering static channels with fixed channel gains.

In this paper, we consider a cooperative jamming scenario with multiple relays and, and we study the optimal relay power allocation problem, specifically under *individual* power constraints per relay and *time-varying* wireless channel conditions. We consider the two cases: (1) when all instantaneous channel gains are known at the source node, i.e., the source node has full channel state information (CSI), (2) when the instantaneous gains of the channels towards the destination node and the relay nodes are known at the source node, but only the *statistics* of the source-eavesdropper and relay-eavesdropper channels are available, i.e., the source node has partial CSI. We solve the power optimization problem via the primal-dual approach for both cases. We derive a closed form solution for the full CSI case, and we propose a gradient update algorithm for obtaining the optimal relay power assignments for partial CSI case. By the primal dual approach, the optimal solution can be re-obtained adaptively for time-varying wireless conditions. The gradient update algorithm is also shown to converge fastly.

The rest of the paper is organized as follows. In section II, we present the system model and the secrecy rate for full and partial CSI cases. In section III, we formulate the primal-dual algorithm for cooperative jamming and we derive the optimal solution for the full CSI case. In Section IV, we investigate the cooperative jamming problem for the partial CSI case and we propose the gradient update algorithm. Section V presents our performance results under different scenarios, and Section VI involves our concluding remarks.

II. System Model

We consider a wireless network, where a source node wants to communicate with a destination node in the presence of an eavesdropper node, and n relay nodes are helping the source with cooperative jamming as depicted in Fig. 1. The eavesdropper is a passive attacker, whose goal is to interpret the source information without trying to modify it. All channels undergo quasi-static flat Rayleigh fading, in which the channel gain remains constant within a time slot and varies independently from slot to slot. For a time slot k, $h_{SD}(k)$ denotes the gain of the channel between the source and the destination nodes, referred to as the main channel; $h_{SJ}(k)$ is the gain of the source-eavesdropper channel, referred to as the eavesdropper channel; $h_{R_iJ}(k)$ and $h_{R_iD}(k)$ denote the gains of the channels from the relay node i to the eavesdropper and destination node respectively, referred to as the relay channels. Due to Rayleigh fading, all channel gains are exponentially distributed, and for all channels additive white gaussian channel noise is assumed with variance σ^2.

We first consider the case when the full channel state information (CSI) is available priori, i.e., all the channel gains are known for each time slot k. Later, we relax this assumption, and consider the case when only the partial CSI is available, i.e., the instantaneous gains of all channels to the destination node are available, but only the statistics of the gain of the channels towards the eavesdropper node are available at the source node.

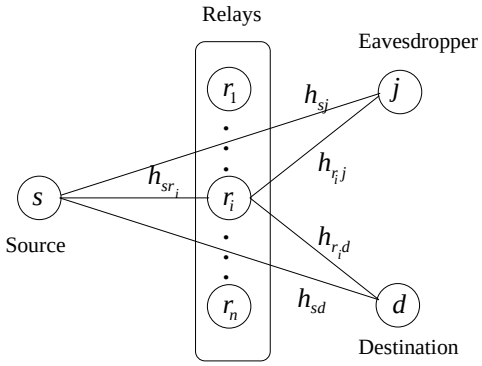

Fig. 1. Network Model for Cooperative Jamming

A. Secrecy Rate with Full CSI

We first review Wyner codes, where the main idea is to introduce randomness to increase secrecy. This idea relies on the fact that the codes make use of random channel errors (due to noise, etc.) to make sure that information obtained by the eavesdropper is not adequate to decode the transmitted message. Let $C(R(k),R_s(k),N)$ denote a Wyner code of size $2^{NR(k)}$ to convey a privacy message set $W = (1,2,...,2^{NR_s(k)})$ in time slot k. The stochastic encoder at the source node selects a private message, $w \in W$, out of $2^{N(R(k)-R_s(k))}$ messages independently at random and sends a codeword a^N. This operation is called random binning [1]. In the last part, decoders at the base station and all other nodes map their received output to a private decoded message $w' \in W$.

Let the vector of symbols received by the eavesdropper be b_e. The following constraint must satisfied by the source to achieve perfect privacy,

$$\frac{1}{N} I(w;b_e) \leq \varepsilon, \tag{1}$$

where $I(w;b_e)$ is the mutual information between private message, w, of the source and received signal, b_e, of the eavesdropper. As $N \to \infty$, the achievable *secrecy rate*, $R_s(k)$, in time slot k is given as:

$$R_s(k) = [R(k) - R_e(k)]^+ \tag{2}$$

where $[x]^+ = \max(0,x)$. Here, $R(k)$ denotes the instantaneous achievable rate for the main channel, which is the mutual information between the channel between the source and destination in time slot k. Likewise, $R_e(k)$ corresponds the mutual information between the channel input at the source and the channel output at the eavesdropper.

Defining P_s as the transmission power of the source node and $P_i(k)$ as the transmission power of relay i in time slot k, $R(k)$ and $R_e(k)$ are calculated as [5]:

$$R(k) = \log\left(1 + \frac{P_s h_{SD}(k)}{\sigma^2 + \sum_i h_{R_i D}(k) P_i(k)}\right), \tag{3}$$

and

$$R_e(k) = \log\left(1 + \frac{P_s h_{SJ}(k)}{\sigma^2 + \sum_i h_{R_i J}(k) P_i(k)}\right), \tag{4}$$

where all instantaneous channel gains are known for all k, which is a valid assumption when all nodes in the system,

including the eavesdropper, have data to be transmitted, and all transmissions can be monitored and all channels can be estimated. This is applicable particularly in networks combining multicast and unicast transmissions, where terminals play dual roles as legitimate receivers for some signals and eavesdroppers for others.

B. Secrecy Throughput with Partial CSI

Unlike the main communication channel which can be estimated at the destination prior to data transmission, sometimes the eavesdropper channel can be hard to predict, in particular when the eavesdropper does not participate in communication but passively listens to the channel. In such cases, at best, the source and the relay nodes can guess the location of the eavesdropper and estimate the statistics of their channel to this node.

For the partial CSI case, due to absence of the instantaneous gains of the eavesdropper channels, one cannot choose the code rate pair utilized in Wyner code, $C(R(k),R_s(k),N)$ to realize perfect secrecy. Instead, and in-advance secrecy rate is used in each time slot k, denoted as $\hat{R}_s(k)$. However, this leads to secrecy outages. When $R(k)-\hat{R}_s(k)<R_e(k)$, perfect secrecy constraint (1) is violated in time slot k. Specifically, $R(k)-\hat{R}_s(k)$ is the rate of the randomization message the source uses in the random binning scheme for secrecy in time slot k, and if the actual rate of the eavesdropper in time slot k, $R_e(k)$, is larger than the randomization rate, we say that *secrecy outage* has occurred. The *probability of secrecy outage* in time slot k is given by

$$P_{s,\text{out}}(k)=\mathbb{P}\left(R(k)-\hat{R}_s(k)<R_e(k)\right). \tag{5}$$

In the event of a secrecy outage, the secretly encoded message is intercepted by the eavesdropper and it cannot be considered as a private transmission. We define the *secrecy throughput* as the rate of information transferred to the destination without secrecy outage, and we calculate it as follows:

$$R_{s,\text{th}}(k)=\hat{R}_s(k)\left(1-P_{s,\text{out}}(k)\right). \tag{6}$$

III. Cooperative Jamming with Full CSI

Given the full CSI, our aim is to maximize the average secrecy rate by properly allocating the power of each relay under average power constraint per relay. Our optimization problem is expressed as

$$\max_{P_i}\mathbb{E}\left[R_s(k)\right]\ \text{ s.t. }\bar{P}_i(k)\leq\alpha_i\quad\forall i, \tag{7}$$

where $R_s(k)$ calculated as in (2). Time averaging is considered and α_i is the maximum average transmit power of relay i.

For solving the secrecy rate maximization problem, we consider the Lagrangian approach and the dual objective, as the optimization tool to solve the optimization problem in (7) [9]. Defining the power of n relays at slot k as, $\mathbf{P}(k)=[P_1(k)\ P_2(k)\ ...\ P_n(k)]$, and the Lagrange multipliers of the dual of the problem as, $\mu(k)=[\mu_1(k)\ \mu_2(k)\ ...\ \mu_n(k)]$, the Lagrangian of (7) is given by

$$L(\mathbf{P}(k),\mu(k))=R_s(k)-\sum_i\mu_i(k)\left(P_i(k)-\alpha_i\right) \tag{8}$$

where $\mu(k)\geq 0$ is the Lagrange multiplier. Then, the dual objective function can be written as,

$$G(\mu(k))=\max_{\mathbf{P}(k)}L(\mathbf{P}(k),\mu(k)), \tag{9}$$

and accordingly, the dual problem is given by

$$\min_{\mu(k)} G(\mu(k)) \tag{10}$$

In this formulation, $\mu(k)$ can be interpreted as the power price vector for the relays. When the relay power, $P_i(k)$, exceeds α_i, its price $\mu_i(k)$ is increased, otherwise $\mu_i(k)$ is reduced.

We now devise a primal-dual algorithm to find the optimal power levels and the prices. More specifically, the powers and prices are updated in such a way that the Lagrangian is maximized with respect to P_i's for the primal objective function, and minimized with respect to $\mu_i(k)$'s for the dual.

We first consider optimizing the Lagrangian function with respect to $\mathbf{P}(k)$. Note that, the Lagrangian function is not a concave function with respect $\mathbf{P}(k)$, due to the existence of power variables in the denominators. In what follows, we show that for the Lagrangian function to be maximized, for any given $\mu(k)$, allowing the transmission of only one relay is optimal. This reduces the dimensionality of the problem and yields simpler analysis to investigate the optimal point.

Proposition 1: In the optimal power control policy, $\mathbf{P}^*(k)$ that maximizes (8) per time slot k, *only one* relay is to transmit, with a non-zero power, i.e., $P_{i^*}(k) > 0$ and $P_j(k) = 0, \forall j \neq i^*$, where i^* is the optimal relay.

Proof Let us first analyze the case when there are only two relays and let us arbitrarily fix the total power level as P, the power allocated to relay 1 as $P_1(k)$ and the power allocated to relay 2 as $P_2(k) = P - P_1(k)$. Next, we will generalize this result for a number of n relays. The partial derivatives of (8) with respect to $P_1(k)$ and $P_2(k)$ are obtained as:

$$\frac{\partial L}{\partial P_1(k)} = -\frac{P_s h_{SD}(k)(h_{R_1D}(k) - h_{R_2D}(k))}{(P_s h_{SD}(k) + A)A} + \frac{P_s h_{SJ}(k)(h_{R_1J}(k) - h_{R_2J}(k))}{(P_s h_{SJ}(k) + B)B} - \mu_1 + \mu_2 \tag{11}$$

$$\frac{\partial L}{\partial P_2(k)} = \sum_i -\frac{P_s h_{SD}(k)(h_{R_2D}(k) - h_{R_1D}(k))}{(P_s h_{SD}(k) + A)A} + \frac{P_s h_{SJ}(k)(h_{R_2J}(k) - h_{R_1J}(k))}{(P_s h_{SJ}(k) + B)B} - \mu_2 \tag{12}$$

where $A = \sigma^2 + P_1(k)h_{R_1D}(k) + (P - P_1(k))h_{R_2D}(k)$ and $B = \sigma^2 + P_1(k)h_{R_1J}(k) + (P - P_1(k))h_{R_2J}(k)$. As clearly seen in (11) and (12), $\frac{\partial L}{\partial P_1(k)} = -\frac{\partial L}{\partial P_2(k)}$. Therefore, either (11) or (12) is monotonically decreasing. Thus, the Lagrangian is maximized either when $P_1(k) = 0$ or $P_2(k) = 0$.

In order to extend the analysis for arbitrary number of relays, let us define $\mathcal{N}$ as the set of n active relays, where a relay is active when it is assigned a non-zero transmit power. Again, assuming fixed total power, P, it is possible to find a relay m, whose transmission power is $P_m(k) = P - \sum_{i \neq j} P_i(k)$, where $P_i(k)$ is the transmit power of relay i. The partial derivative of (8) with respect to $P_i(k)$ is:

$$\frac{\partial L}{\partial P_i(k)} = -\frac{P_s h_{SD}(k)(h_{R_iD}(k) - h_{R_nD}(k))}{(P_s h_{SD}(k) + A')A'} + \frac{P_s h_{SJ}(k)(h_{R_iJ}(k) - h_{R_nJ}(k))}{(P_s h_{SJ}(k) + B')B'} - \mu_i(k) \tag{13}$$

where $A' = \sigma^2 + \sum_{i \neq m} P_i(k)h_{R_iD}(k) + (P - \sum_{i \neq m} P_i(k))h_{R_mD}(k)$ and $B' = \sigma^2 + \sum_{i \neq m} P_i(k)h_{R_iJ}(k) + (P - \sum_{i \neq k} P_i(k))h_{R_mJ}(k)$. Obviously, the partial derivatives of (8) with respect to $P_m(k)$ is

$$\frac{\partial L}{\partial P_m(k)} = -\sum_{i \neq m} \frac{\partial L}{\partial P_i(k)} \tag{14}$$

Here, the relay m satisfies $\frac{\partial L}{\partial P_m(k)} > 0$ and consequently, we have $\frac{\partial L}{\partial P_i(k)} < 0$. This result suggests that at the optimal point, $P_m(k) = 0$. Relay m can be interpreted as the relay, which has the least possible contribution for increasing

the secrecy rate due to jamming. In the next step, we reduce the active set to $\mathscr{N}-\{m\}$, and we conduct the same analysis over this set, $\mathscr{N}-\{m\}$. In each step, we find out that there is a relay whose transmit power is equal to zero at the optimal point. In the last step, when only two relays are left in the active set, we conduct the above analysis for two relays. As a result, by induction, it is shown that at the optimal point, only one relay has non-zero allocated power. ■

The significance of Proposition 1 is that, for a given channel state in time slot k, the achievable secrecy rate can be obtained in closed form. From the application point of view, the source will separately compute the optimal power for each relay, with the condition that the other relays have zero transmit power. Then, it will select the relay whose optimal power maximizes the Lagrangian function in (8).

Next, we find the optimal power level for each relay. Considering relay i and by differentiating (8) with respect to P_i, we get

$$\begin{aligned}\frac{\partial L}{\partial P_i(k)} = &-\frac{P_s h_{SD}(k) h_{R_iD}(k)}{(P_s h_{SD}(k)+\sigma^2+P_i(k)h_{R_iD}(k))(\sigma^2+P_i(k)h_{R_iD}(k))} \\ &+\frac{P_s h_{SJ}(k) h_{R_iJ}(k)}{(P_s h_{SJ}(k)+\sigma^2+P_i(k)h_{R_iJ}(k))(\sigma^2+P_i(k)h_{R_iJ}(k))}-\mu_i(k)\end{aligned} \tag{15}$$

For obtaining the roots of the above equation, we solve the fourth order polynomial equation below:

$$F_{i,4}P_i(k)^4+F_{i,3}P_i(k)^3+F_{i,2}P_i(k)^2+F_{i,1}P_i(k)+F_{i,0}=0, \tag{16}$$

where

$$\begin{aligned}F_{i,4} &= h_{R_iD}(k)h_{R_iJ}(k) \\ F_{i,3} &= h_{R_iD}(k)h_{R_iJ}(k)(P_s h_{SD}(k)+2\sigma^2)+h_{R_iD}(k)h_{R_iJ}(k)(P_s h_{SJ}(k)+2\sigma^2) \\ F_{i,2} &= h_{SJ}(k)h_{R_iD}(k)-h_{SD}(k)h_{R_iJ}(k)-(P_s h_{SJ}(k)+\sigma^2)\sigma^2 h_{R_iD}(k) \\ &\quad -(P_s h_{SD}(k)+\sigma^2)\sigma^2 h_{R_iJ}(k)-h_{R_iD}(k)h_{R_iJ}(k)(P_s h_{SJ}(k)+2\sigma^2)(P_s h_{SD}(k)+2\sigma^2) \\ F_{i,1} &= h_{SJ}(k)h_{R_iD}(k)(P_s h_{SD}(k)+2\sigma^2)-h_{SD}(k)h_{R_iJ}(k)(P_s h_{SJ}(k)+2\sigma^2) \\ F_{i,0} &= -\mu_i(k)(P_s h_{SD}(k)+\sigma^2)(P_s h_{SJ}(k)+\sigma^2)\sigma^4\end{aligned} \tag{17}$$

The solution of the quadratic equation in (16) can be expressed in closed form as given in [14]. The gradient of $L(\mathbf{P}(k),\mu(k))$ with respect to $\mu_i(k)$ is obtained as:

$$L_{\mu_i(k)}(\mathbf{P}(k),\mu(k))=\alpha_i-P_i(k), \tag{18}$$

and the optimal solution is obtained by solving (16) and (18).

Finally, for updating μ_i's we employ the sub-gradient algorithm, since it has been widely applied in solving Lagrangian problems. The sub-gradient algorithm is a simple and effective method, similar to the gradient descent method, but differently, the sub-gradient method is also applicable to non-differentiable objectives [9]. In our problem, the updates of μ_i's are in the negative direction of the gradient of $L(\mathbf{P}(k),\mu(k))$ in (18) calculated as:

$$\mu_i(k+1)=\left(\mu_i(k)-\varepsilon(k)(\alpha_i-P_i(k))\right)^+, \tag{19}$$

where $[x]^+=\max(0,x)$ and $\varepsilon(k)\geq 0$ is the step size. The convergence of the sub-gradient algorithm is shown in

[12] for a arbitrarily small step sizes.

Summarizing our cooperative jamming solution, for each time slot k, the source node calculates the transmit power, $P_i(k)$, of each relay i, based on the channel gains and the Lagrange multipliers, $\mu_i(k)$. The relay, which maximizes the Lagrangian function in (8), is selected, and other relays are set to have zero transmit power. The Lagrange multipliers are updated based on equation (19).

IV. Cooperative Jamming with Partial CSI

In this section, we investigate the cooperative jamming scenario when only partial CSI is available, when the statistics of the channels from the source to the eavesdropper and from the relays to the eavesdropper are given at the source node.

As explained in Section II. B, a secrecy outage event takes place, when the eavesdropper has obtained more information than the randomization rate in a privately encoded message. In time-varying wireless channels, a channel outage occurs when the received signal to interference/noise ratio drops below a threshold necessary for decoding the transmitted signal. Likewise, a secrecy outage event occurs, when the randomized information rate drops below the information rate obtained by the eavesdropper. In this case, the amount of randomized bits is not sufficient to confuse the eavesdropper, and the eavesdropper obtains sufficient amount of information to decode the secret packet. In the following, we analyze the secrecy outage probability, $P_{s,\text{out}}(k)$.

Lemma 1: Given the statistics of the channels to the eavesdropper and the chosen secret encoding rate $\hat{R}_s(k)$, the secrecy outage probability, is calculated as:

$$P_{s,\text{out}}(k) = e^{-\sigma^2 \lambda_s D(k)} \left(\sum_i \frac{\lambda_i(k)}{\lambda_i(k) + \lambda_s D(k)} \prod_{j \neq i} \frac{\lambda_j(k)}{\lambda_j(k) - \lambda_i(k)} \right), \tag{20}$$

where $D(k) = 2^{R(k) - \hat{R}_s(k)} - 1$, and $\lambda_i(k) = \frac{1}{P_i(k)\mathbb{E}[h_{R_i J}]}$ for relay i and $\lambda_s = \frac{1}{P_s \mathbb{E}[h_{SJ}]}$ for the source node. Note that, $R(k)$, which is calculated as in (3), solely depends on gain of the channel between the source and the destination and the gains of the relay-destination channels. Since these gains are known per time slot k, $R(k)$ is constant in time slot k. However, since the instantaneous gain of the eavesdropper channel is not known, $\hat{R}_s(k)$ is variable, which affects the secrecy outage probability.

Proof In order to derive the secrecy outage probability, we first need to statistically characterize $R_e(k)$ in (4). We start with the distribution of the sum of independent exponential random variables for the summation in the denominator of the rational term in the log function in (4). Note that, each term in the summation is an exponential random variable, corresponding to each relay's transmission received at the eavesdropper, and recalling that all are independent, we define $(X_i)_{i=1,\ldots,n}$ as independent exponential random variables with distinct respective parameters λ_i. For $n = 2$, the probability density function for the sum is found as [10],

$$f_{X_1+X_2}(x) = f_{X_1}(x) * f_{X_2}(x) = \int_0^x \lambda_1 e^{-\lambda_1 (x-u)} \lambda_2 e^{-\lambda_2 x} du = \lambda_1 \lambda_2 \frac{e^{-\lambda_2 x} - e^{-\lambda_1 x}}{\lambda_1 - \lambda_2}. \tag{21}$$

Considering $n \geq 3$, by induction, we can obtain,

$$\begin{aligned} f_{X_1+X_2+...X_n}(x) &= f_{X_1+X_2+...X_{n-1}}(x) * f_{X_n}(x) = \left[\prod_{i=1}^{n-1}\lambda_i\right]\sum_{j=1}^{n-1}\frac{e^{-\lambda_j x}}{\prod_{k\neq j}\lambda_k-\lambda_j} * f_{X_n}(x) \\ &= \left[\prod_{i=1}^{n-1}\lambda_i\right]\sum_{j=1}^{n-1}\frac{e^{-\lambda_n x}-e^{-\lambda_j x}}{(\lambda_j-\lambda_n)\prod_{k\neq j}\lambda_k-\lambda_j} \\ &= \left[\prod_{i=1}^{n}\lambda_i\right]\sum_{j=1}^{n}\frac{e^{-\lambda_j x}}{(\lambda_j-\lambda_n)\prod_{k\neq j}\lambda_k-\lambda_j}, x>0. \end{aligned} \tag{22}$$

Next, we define a new random variable Y, as $Y = X_1 + X_2 + ... + X_n + \sigma^2$, where X_i denotes the signal received from relay i and σ^2 denotes the constant noise variance. Then, $f_Y(y)$ is obtained as:

$$f_Y(y) = \left[\prod_{i=1}^{n}\lambda_i\right]\sum_{j=1}^{n}\frac{e^{-\lambda_j(y-\sigma_2)}}{(\lambda_j-\lambda_n)\prod_{k\neq j}\lambda_k-\lambda_j}, y>\sigma^2. \tag{23}$$

Now, let Z be the random variable for the numerator term in (4) due to the transmission from the source to the eavesdropper. We know that Z is also exponential with $f_Z(z) = \lambda_s e^{-\lambda_s z}$, where $\lambda_s = \frac{1}{P_s\mathbb{E}[h_{SJ}]}$. Now, re-writing the definition in (5), we are ready to calculate the secrecy outage probability,

$$\begin{aligned} P_{s,\text{out}}(k) &= \mathbb{P}\left(R(k) - \hat{R}_s(k) < \log\left(1+\frac{Z}{Y}\right)\right) \\ &= \mathbb{P}\left(D(k) < \frac{Z}{Y}\right) = \mathbb{P}\left(D(k)Y < Z\right) \end{aligned} \tag{24}$$

where $D(k) = 2^{R(k)-\hat{R}_s(k)} - 1$. Since the random variables Y and Z are independent, we can calculate this probability as:

$$\begin{aligned} P_{s,\text{out}}(k) &= \int_{y=\sigma^2}^{\infty}\int_{z=D(k)y}^{\infty} f_Y(y) f_Z(z) dy dz \\ &= \int_{y=\sigma^2}^{\infty}\int_{z=D(k)y}^{\infty}\left[\prod_{i=1}^{n}\lambda_i\sum_{j=1}^{n}\frac{e^{-\lambda_j(y-\sigma_2)}}{\prod_{k\neq j}\lambda_k-\lambda_j}\right]\lambda_s e^{-\lambda_s z} dy dz \\ &= \int_{y=\sigma^2}^{\infty}\left[\prod_{i=1}^{n}\lambda_i\sum_{j=1}^{n}\frac{e^{-\lambda_j(y-\sigma_2)}e^{\lambda_s y D(k)}}{(\lambda_j-\lambda_n)\prod_{k\neq j}\lambda_k-\lambda_j}\right] dy \\ &= \left[\prod_{i=1}^{n}\lambda_i\sum_{j=1}^{n}\frac{e^{-\lambda_j(y-\sigma_2)}e^{\lambda_s y D(k)}}{\prod_{k\neq j}\lambda_k-\lambda_j} - \frac{1}{\lambda_j+\lambda_s D(k)}\right]|_{\sigma^2}^{\infty} \\ &= e^{-\lambda_s D\sigma^2}\prod_{i=1}^{n}\lambda_i\sum_{j=1}^{n}\frac{1}{\prod_{k\neq j}\lambda_k-\lambda_j}\frac{1}{\lambda_j+\lambda_s D} \end{aligned} \tag{25}$$

After simplifications on (25), we obtain the result in Lemma 1. This has concluded the proof. ■

Proposition 2: The following relationship should be satisfied for a relay to improve the secure communication rate:

$$2^{-\hat{R}_s(k)}\frac{P_s h_{SD}(k)}{\sigma^2}\left(\mathbb{E}\left[h_{R_iJ}\right] + h_{R_iD}(k)\right) < \mathbb{E}\left[h_{R_iJ}\right]\left(2^{-\hat{R}_s(k)} - 1\right). \tag{26}$$

The above condition ensures that positive transmit power of relay i decreases the secrecy outage probability.

Otherwise, it only increases the secrecy outage probability and decreases the secrecy throughput.

Proof In order to determine whether a relay i can contribute the source's private transmission, we need to show that the secrecy outage probability is a decreasing function with respect to the transmit power of relay i, $P_i(k)$, which is evaluated at zero. First, we obtain the derivative of $P_{s,\text{out}}(k)$ with respect to $P_i(k)$:

$$\begin{aligned}\frac{\partial P_{s,\text{out}}(k)}{\partial P_i(k)} &= \frac{\partial e^{-\sigma^2\lambda_s D(k)}\left(\frac{\lambda_i}{\lambda_i+\lambda_s D(k)}\right)}{\partial P_i(k)} \\ &= -e^{-\sigma^2\lambda_s D(k)}\sigma^2\lambda_s\frac{\partial D}{\partial P_i(k)}\left(\frac{\lambda_i}{\lambda+\lambda_s D(k)}\right)+e^{-\lambda^2\lambda_s D}\left(\frac{\frac{\partial\lambda_i}{\partial P_i(k)}\lambda_s D(k)-\lambda_i\lambda_s\frac{\partial D(k)}{\partial P_i(k)}}{(\lambda_i+\lambda_s D)^2}\right) \end{aligned} \tag{27}$$

where $\frac{\partial D(k)}{\partial P_i(k)} = -2^{-\hat{R}_s(k)}\frac{Psh_{SD}(k)h_{R_iD}(k)}{(\sigma^2+P_i(k)h_{R_iD}(k))^2}$. If we evaluate the derivative in (27) at $P_i(k)=0$:

$$\frac{\partial P_{s,\text{out}}(k)}{\partial P_i(k)}|_{P_i(k)=0} = \lambda_s 2^{-\hat{R}_s(k)}\frac{Psh_{SD}(k)h_{R_iD}(k)}{\sigma^2} - \mathbb{E}\left[h_{R_iJ}\right]\lambda_s(2^{-\hat{R}_s}(1+\frac{Psh_{SD}(k)}{\sigma^2}-1)<0. \tag{28}$$

In order to increase the secrecy rate of the source, the derivative $\frac{\partial P_{s,\text{out}}(k)}{\partial P_i(k)}|_{P_i(k)=0}$ in (28) should be negative, which means that the secrecy outage probability is a decreasing function of $P_i(k)$. Thus, arranging the terms in (28), we obtain the following relationship:

$$2^{-\hat{R}_s(k)}\frac{P_s h_{SD}(k)}{\sigma^2}\left(\mathbb{E}\left[h_{R_iJ}\right]+h_{R_iD}(k)\right) < \mathbb{E}\left[h_{R_iJ}\right]\left(2^{-\hat{R}_s(k)}-1\right). \tag{29}$$

■

Our objective is to maximize the secret information transmitted to the destination node without secrecy outage, so we want to maximize the secrecy throughput which is defined in (6). Thus, the optimization problem in (7) is modified for the partial CSI case as:

$$\max_{P_i(k)} \mathbb{E}\left[\hat{R}_s(k)(1-P_{s,\text{out}}(k))\right] \text{ s.t. } \bar{P}_i(k)\leq\alpha_i \quad \forall i. \tag{30}$$

We solve this optimization problem again by the Lagrangian approach and the dual objective. Obtaining the Lagrangian as,

$$L(\mathbf{P}(k),\mu(k)) = \hat{R}_s(k)(1-P_{s,\text{out}}(k)) - \sum_i \mu_i(k)\left(P_i(k)-\alpha_i\right) \tag{31}$$

and the dual objective function as,

$$G(\mu(k)) = \max_{\mathbf{P}(k)} L(\mathbf{P}(k),\mu(k)), \tag{32}$$

the dual problem is given by,

$$\min_{\mu(k)} G(\mu(k)). \tag{33}$$

Taking the derivative of $L(\mathbf{P}(k),\mu(k))$ with respect to $P_i(k)$, the gradient is obtained as follows:

$$L_{P_i(k)}(\mathbf{P}(k),\mu(k)) = \frac{\partial\hat{R}_s(k)(1-P_{s,\text{out}}(k))}{\partial P_i(k)} - \mu_i(k)P_i(k),. \tag{34}$$

Similar to the full CSI case, we again propose to use the sub-gradient algorithm for updating μ_i's:

$$\mu_i(k+1) = (\mu_i(k) - \varepsilon(k)(\alpha_i - P_i(k)))^+, \tag{35}$$

where $[x]^+ = \max(0,x)$ and $\varepsilon(k) \geq 0$ is the step size.

Since the function in (34) is highly non-linear with respect to $P_i(k)$, obtaining optimal $P_i^*(k)$ is rather involved. Therefore, we propose to use the gradient algorithm for power assignment as well. Since we analyze the power levels within each time slot, we drop the time slot variable k and the source updates the utilized power P_i from relay i according to the following dynamic equation:

$$\phi_i = \frac{dP_i}{dt} = \dot{P}_i = -\delta_i \frac{\partial L}{\partial P_i} \ \forall i, \tag{36}$$

where δ is a positive step-size. Now, we introduce a smaller scale time unit, l, where the power levels are updated as:

$$P_i^{(l)} = P_i^{(l-1)} + \dot{P}_i^{(l-1)} \ \forall i. \tag{37}$$

By taking the derivative of the Lagrangian in (34) with respect to P_i, we obtain ϕ_i

$$\begin{aligned}\phi_i = {} & e^{-\sigma^2\lambda_s D}\sigma^2\lambda_s \frac{\partial D}{\partial P_i}\cdot\left(\sum_i \frac{\lambda_k}{\lambda_k+\lambda_s D}\prod_{j\neq k}\frac{\lambda_j}{\lambda_j-\lambda_k}\right) \\ & - e^{-\sigma^2\lambda_s D}\left(-\sum_{j\neq i}\frac{\lambda_j}{(\lambda_j+\lambda_s D)^2}\frac{\lambda_j}{\lambda_j-\lambda_i}\frac{\partial D}{\partial P_i} + \sum_{j\neq i}\frac{\lambda_j}{\lambda_j+\lambda_s D}\frac{\lambda_j}{(\lambda_j-\lambda_i)^2}\frac{\partial \lambda_i}{\partial P_i}\right)\end{aligned} \tag{38}$$

where

$$\frac{\partial D}{\partial P_i} = -2^{-\hat{R}_s}\frac{P_s h_{SD} h_{R_i D}}{\left(\sigma^2 + \sum_j P_j h_{R_j D}\right)^2}$$

and $\frac{\partial \lambda_i}{\partial P_i} = -\frac{1}{\mathbb{E}\left[h_{R_i J}\right]P_i^2}$. (38) defines a method for the relays to update their purchased power levels based on the channel gains and the current power levels of the other relays in the system.

V. Simulation Results

In this section, we briefly demonstrate the performance of our proposed algorithms by investigating the secrecy rate under cooperative jamming in comparison to the secrecy rate for transmission without cooperative jamming, which we refer to as direct transmission and to the case when there is no eavesdropper. Capacity simulations are performed according to the following model and parameters: The source power is set as, $P_s = 1$ watt. The noise variance is $\sigma^2 = 10^{-6}$ and the bandwidth is $W = 1$ Hz, for simplicity. We consider Rayleigh fading channels, so the channel gains are exponentially distributed with their means calculated as $E[h^2] = d^{(-c/2)}$, where d is the distance between considered nodes, and c is the path loss exponent (chosen here as $c = 3.5$). In addition, step sizes, ε and δ are selected as 0.01, which are sufficiently small for the algorithms to converge. In all experiments, the average power constraints per relay i are set identically, as $\alpha_i = 0.1 \ \forall i$, unless it is stated otherwise. We consider a linear topology, where all the nodes are placed along a horizontal line. The source node is located at the origin, 0 m. The locations of the eavesdropper node, the relays and the destination node are changed in the experiments as explained next.

In the first set of experiments, we evaluate the secrecy rate considering our proposed optimal power allocation solution with CJ, when full CSI is available. With the source node at 0 m., the eavesdropper node is placed at 40 m., and ten relays are randomly placed within (20-30) m. from the source node, we let the location of the destination

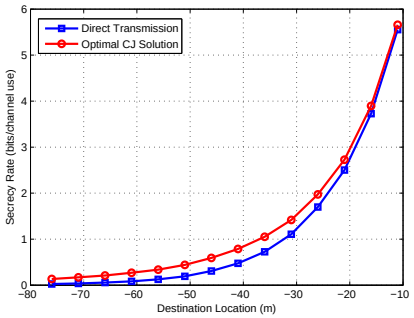

Fig. 2. Secrecy rate versus source-destination distance

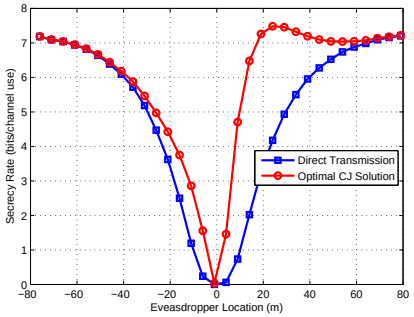

Fig. 3. Secrecy rate versus eavesdropper location

node vary from -10 m. to -80 m. from the source node. We obtain the secrecy rate curve as shown in Fig. 2, where it is shown that the secrecy rate of the direct transmission is increased significantly, by $\%20 - \%80$, when CJ is employed with our optimal power assignment algorithm. Another important observation is that, in direct transmission, when the source-destination distance is increased, the secrecy rate becomes smaller approaching zero, as the eavesdropper channel becomes more favorable than the destination channel. However, even in such challenging cases, utilizing CJ with our power assignment scheme results in a non-zero secrecy rate. We have also investigated the secrecy rate as we varied the location of the destination from 10 m to 80 m, and we observed that the effect of cooperative jamming is decreased as the destination node gets closer to the relays.

In the second experiment, the source node is placed at 0 m, the location of the destination node is fixed as -10 m., and we vary the location of the eavesdropper node from -80 m. to 80 m. Again, ten relays are randomly placed within (20-30) m. from the source node. We obtain the secrecy rate as seen in Fig. 3, where the CJ solution again outperforms direct transmission. We also observe that, as the eavesdropper gets closer to the relay nodes, the contribution of the relay nodes to the secrecy rate is increased. This is due to the fact that cooperative jamming can deteriorate the information obtained by the eavesdropper more efficiently.

Finally, we investigate the effect of the number of relays on the secrecy rate. With the source at 0 m., the destination node at -10 m. and the eavesdropper node at 40 m., we vary the number of relays, which are all co-located at 25 m. Our results in Fig. 4 depict that, as the number of relays is increased, the secrecy rate obtained by cooperative jamming is increased significantly up to around five relays, and afterwards we observe diminishing returns. Naturally, the secrecy rate of the direct transmission remains the same at a level. In addition, as the number of relays increases, the secrecy rate approaches to the rate when there is no eavesdropper in the network.

In the last experiment for the full CSI case, we observe the effect of average power constraint, $\alpha_i = \alpha \ \forall i$, on

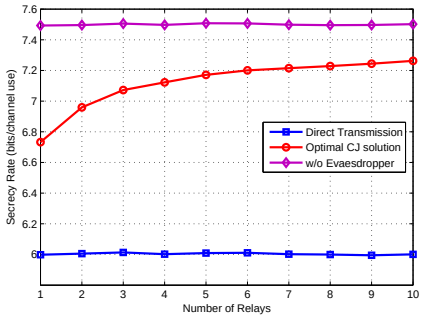

Fig. 4. Secrecy rate versus the number of relays

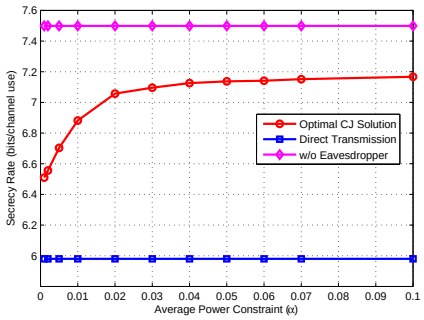

Fig. 5. Secrecy rate versus the average power constraint

the secrecy rate. All nodes are placed in the same locations as in the previous experiment except the number of relays is set as five. As seen in Fig. 5, the secrecy rate is increased with the average power constraint, as expected. Starting around $\alpha = 0.1$, the power constraint becomes inactive, since the constraint is realized with equality.

Next, we investigate the performance of our proposed algorithms for CJ with partial CSI. First, we observe the convergence of the gradient update algorithm described in Section IV. The source node in the linear topology is located at 0 m., the eavesdropper node is at 40 m and the destination is at -10 m. In addition, five relays are randomly located between (20-30) m. As seen in Fig. 6, the transmit power levels of the five relay nodes exhibit fast convergence, and the optimal solution is attained within a few iterations.

In the second experiment, we observe the secrecy rate as the location of the destination node is varied. The source node is again placed at 0 m., the destination node is at -10 m. and we vary the location of the eavesdropper node from -80 m. to 80 m. Five relays are randomly located between (20-30) m. For these experiments, $\hat{R}_s(k)$ is set as $\hat{R}_s(k) = 6$ for all time slots. As seen in Fig. 7, cooperative jamming improves the secrecy throughput even when only the partial CSI is available at source node.

VI. Conclusions

In this paper, we have investigated the cooperative jamming approach with optimal power allocation for improving the secure rate of wireless channels, by considering both ideal and more realistic conditions, with full CSI and partial CSI, respectively. We formulate the power assignment problem via a primal-dual algorithm, considering individual power constraints on the relays and time-varying channel conditions. For the full CSI case, we derive the allocated power levels in closed form, and we propose a gradient update algorithm for obtaining optimal solutions for the partial CSI case. Via simulations, we show that cooperative jamming with our optimal power assignment

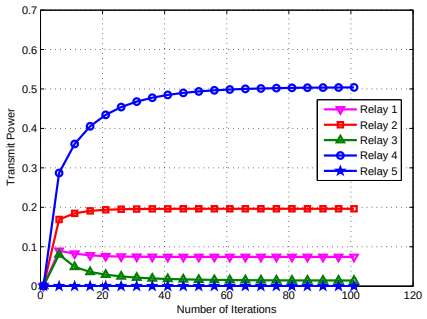

Fig. 6. Convergence of gradient update algorithm

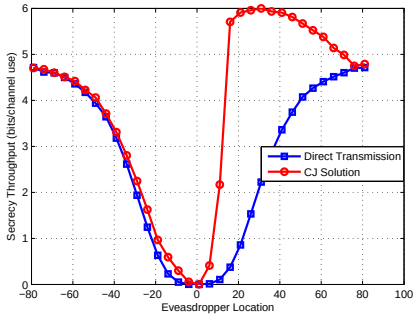

Fig. 7. Secrecy throughput versus eavesdropper location(Partial CSI Case)

algorithm increases the secrecy rate by $\%20 - \%80$ over the direct transmission.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355138, Oct. 1975.

[2] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messsages," IEEE Transactions on Information Theory, vol.24, pp. 339-348, May 1978.

[3] L. lai, H. El Gamal, and H. V. Poor, "Secure Commuunication over Fading Channels," IEEE Transactions on Information Theory, vol. 54, pp. 2470-2492, June 2008.

[4] A. Khisti and G. W. Wornel, "Secure Transmissions with Multiple Antennas: The MISOME Wiretap Channel", IEEE Transactions on Information Theory, vol. 7, pp. 3088-3014, July 2010.

[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, March 2010.

[6] J. Zang and M. C. Gursoy,"Collaborative Relay Beamforming for Secrecy, Dec. 2009.

[7] J. Li, A. P. Petropulu, and S. Weber, "Optimal Cooperative Relaying Schemes for Improving Wireless Physical Layer Security,", IEE Transactions on Signal Processing, vol. 59, no. 7, 2011.

[8] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relay", IEE Transactions on Signal Processing, vol. 59, no.3, March 2011.

[9] D. P. Bertsekas, Nonlinear Programming. Cambridge: *Athena Scientific*, 1999.

[10] E. T. Jaynes, Probability Theory. *Cambridge University Press*, 2003

[11] Khalil, H.K. (1996). Nonlinear systems. Prentice Hall Upper Saddle River, NJ.

[12] S. H. Low, D. E. Lapsley, "Optimization Flow Control, I: Basic Algorithm and Convergence," IEEE Transactions on Networking, vol. 7, pp. 861-874, Dec. 1999.

[13] X. Tang, R. Liu, P. Spasojevic and H. V. Poor, "On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-Fading Channels", IEEE Trans. Inform. Theory, vol.55, no. 4, pp. 1575-1591, March 2009.

[14] I. N. Stewart, Galois Theory, 3rd. ed., Chapman and Hall/CRC Mathematics, Boca Raton, FL, 2004.

[15] D. P. Palomar and M. Chiang, “A Tutorial on Decomposition Methods for Network Utility Maximization”, IEEE Journal on Selected Areas in Communications, vol. 24, no. 8, pp. 1439-1451, Aug. 2006.