Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper

Lun Dong   Homayoun Yousefi'zadeh   Hamid Jafarkhani
Center for Pervasive Communications and Computing
University of California, Irvine
[lund,hyousefi,hamidj]@uci.edu

***Abstract*—Relying on physical layer security is an attractive alternative of utilizing cryptographic algorithms at upper layers of protocol stack for secure communications. In this paper, we consider a two-hop wireless relay network in the presence of an eavesdropper. Our scenario of interest spans over a four-node network model including a source, a destination, a trusted relay, and an untrusted eavesdropper in which the relay forwards the source message in a decode-and-forward (DF) fashion. The source and relay are allowed to use some of their available power to transmit jamming signals in order to create interference at the eavesdropper. The relay and destination are assumed to have the knowledge of the jamming signals. An important question is how to allocate the transmission power of the message signal and that of the jamming signal. First, we propose an optimal power allocation solution in which the knowledge of global channel state information (CSI) is required. To facilitate practical system design, two simple yet sub-optimal power allocation solutions are proposed which do not rely on eavesdropper's channels. For the purpose of performance comparisons, power allocation problems for two benchmark schemes without jamming are also analyzed.**

Index Terms: Physical Layer Security, Secrecy Rate, Jamming, Wireless Relay Networks, Decode-and-Forward.

I. Introduction

Due to the broadcast nature of the wireless medium, transmitting confidential information securely in presence of possible eavesdroppers is of increasing importance. Traditionally, the issue of information secrecy has been primarily addressed at the upper layers of the protocol stack via the use of cryptographic algorithms. However, there are several significant challenges for cryptographic approaches in wireless networks, e.g., private key management complexity, key distribution obstacles, and key transmission security issues [1]. Recently, there has been a growing interest in implementing wireless security at the physical (PHY) layer, which exploits the physical characteristics of the wireless channel to transmit information securely [2]. In wireless PHY security, the figure of merit is *secrecy rate* defined as the rate at which information can be transmitted secretly from a source to its intended destination. The maximum achievable secrecy rate is named the *secrecy capacity*. For a Gaussian channel, the achievable secrecy rate equals to the difference between the mutual information accumulated at the destination and that accumulated at the eavesdropper which is not less than zero [3].

Recently, cooperative jamming has emerged as a promising technique to enhance wireless PHY secrecy [4]. The basic idea is to send proper jamming signals in order to create interference at an eavesdropper. In traditional wireless communications, interference is typically undesired and shall be mitigated or avoided. However, intentional creation of interference is of special interest in secure communications. In this paper, our focus is to enhance wireless PHY secrecy for two-hop wireless relay networks by using jamming strategies. It is well understood that the use of relaying techniques can introduce significant benefits for wireless networks [5]-[7]. Our focus in this paper is decode-and-forward (DF) relaying. Other relaying strategies such as amplify-and-forward (AF) will be the subject of our future work. We consider a two-hop DF-based relay network in the presence of an eavesdropper. The network consists of a source, a destination, a trusted relay, and an untrusted eavesdropper each equipped with a single antenna. The trusted relay forwards the source message to the destination in a DF fashion. There is no direct link between the source and the destination. Our main contributions are briefly described below.

In addition to transmitting the message signal, source and relay are allowed to use some of their available power to transmit jamming signals. We assume that a legitimate receiver (relay or destination) has an apriori knowledge of the jamming signal, which could be implemented in practice with a small amount of overhead. Jamming signals can then create interference at the eavesdropper, but be completely removed at legitimate receivers, thereby enhancing wireless secrecy. An important problem is how to allocate the power for transmitting the message signal and the jamming signal. We analyze the optimal power allocation problem and show that solving it requires the global channel knowledge. Considering the fact that the eavesdropper's channel knowledge may not be available in practical scenarios, we propose two simple but sub-optimal power allocation solutions that do not rely on the knowledge of eavesdropper's channels. We also analyze power allocation problems of two benchmark schemes without jamming. While the first benchmark scheme corresponds to traditional DF relaying without eavesdropper, the second benchmark takes into account the presence of an eavesdropper.

This work was sponsored in part by a research grant from the Boeing Company.

A. Related Work

In this subsection, we briefly review some of the recent representative work most closely related to our work and then differentiate our work from the existing work. In [8], a four-node system model including source, destination, eavesdropper, and relay is considered in which the relay transmits an artificial noise independent of the source signals in order to confuse the eavesdropper. In [9], the secrecy rate of orthogonal relay eavesdropper channels is studied. Both relay and destination nodes receive the source signals on two orthogonal channels, the destination also receives transmissions from the relay on its channel, and the eavesdropper overhears either one or both of the orthogonal channels. In [10], a relay is used for helping the eavesdropper to degrade the secrecy rate. In [11], an extra jammer is introduced to enhance the secrecy performance for an AF-based relay network. In [12], artificial jamming noise is added to achieve secrecy for two scenarios: one in which the source has multiple antennas and the other in which the source has a single antenna but multiple helpers are available. The work of [13] considers the case of a multi-antenna relay in which the relay sends jamming signals based on a beamforming strategy.

In most of the above cases, a relay is utilized to only *either* forward the source information *or* send a jamming signal. For the former case, the source-to-relay communication is not protected from eavesdropping, while in the latter one, the system cannot enjoy the benefits of relaying. To the best of our knowledge, cooperative jamming for protecting communications in both phases of relay networks has not been studied before. In this work, both relaying and jamming are taken into account, so communications in both phases could be protected from eavesdropping. Also, our jamming strategies and design problems are different from existing works. More specifically, in this work we consider power allocation problems to maximize the secrecy rate subject to a per-node power constraint.

II. System Model and Jamming Strategy

As the system model, we utilize a four node network. They are namely a source (S), a destination (D), a trusted relay (R), and an untrusted eavesdropper (E). Each node is equipped with a single omni-directional antenna and operates in a half-duplex mode. We assume that there is no direct $S \rightarrow D$ link. To deliver a source message to the destination, the source first transmits its message to the relay (Phase 1), and the relay then forwards the message to the destination in a DF fashion (Phase 2). Wireless transmissions in both phases could be eavesdropped. The eavesdropper is passive and its goal is to interpret the source information without trying to modify it. Our objective is to improve the wireless secrecy via transmitting appropriate jamming signals. There is no extra jammer but an apriori knowledge of jamming signals is available at legitimate receivers. To enhance secrecy, we allow the source and the relay to use some of their power to transmit a jamming signal, in addition to transmitting the message signal. The system model is illustrated in Fig. 1.

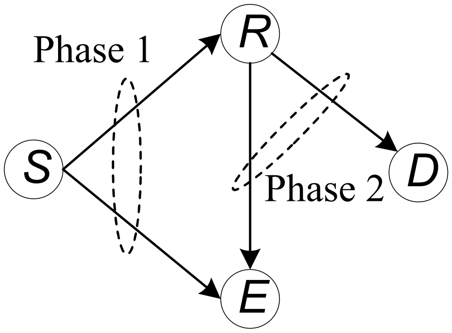

Fig. 1. An illustration of the system model.

As the secrecy capacity for a general relay channel remains to be an open problem even in the absence of secrecy constraints, this work focuses on the achievable secrecy rate. This translates to deriving the lower bounds of the secrecy capacity similar to the literature works of [8], [10], [13], and [14]. The achievable secrecy rate R_{sec} is defined as [10]:

$$R_{sec} = [R_D - R_E]^+ \tag{1}$$

where R_D is the accumulated rate at the destination, R_E is the accumulated rate at the eavesdropper, and $[x]^+$ denotes $\max(x, 0)$. This secrecy rate can be achieved via the use of Gaussian inputs.

The goal of the jamming signal is to create interference at the eavesdropper in order to reduce R_E. Notice that the relay has an apriori knowledge of the jamming signal sent by the source, and the destination has an apriori knowledge of the jamming signals sent by the relay. This can be implemented in practice with a small amount of overhead. For example, the jamming signal can be a Gaussian noise generated by a pseudo-random generator with finite states, and the trusted nodes maintain the same pseudo-random generator. Only the state of the pseudo-random generator needs to be sent to the relay (for Phase 1) or destination (for Phase 2) via a separate and secure control channel. In this way, legitimate receivers have the complete knowledge of jamming signals.

We also assume that the channels are quasi-static and the channel knowledge is available, and as such the jamming signals can be completely removed from the signal received at legitimate receivers. Although the jamming signal does not create interference at relay or destination, under a per-node power constraint the power for transmitting the message signal is reduced, resulting in decreasing R_D. Clearly, there is a tradeoff between transmitting the message and jamming signal. The power allocation problem is thus of interest.

We consider a practical transmit power constraint in which the transmit power at each node is limited to an upper bound. P_S and P_R are the total power budget of the source and the relay, respectively. Thermal noise at any node is assumed to be zero-mean white complex Gaussian with variance σ^2, i.e., $\mathcal{CN}(0, \sigma^2)$. We denote $h_{i,j}$ as the flat fading channel for the $i \rightarrow j$ link. For example, $h_{S,R}$ is the channel between the source and the relay.

Noticing that the jamming signals only interfere with the eavesdropper, increasing jamming power always improves the secrecy rate. The source or the relay shall always use all their available power for maximizing the secrecy rate. Let us denote αP_S ($0 \leq \alpha \leq 1$) to be the power allocated by the source for transmitting its message, and βP_R ($0 \leq \beta \leq 1$) to be the power allocated by the relay for transmitting the source message. The power allocated for transmitting the jamming signal for the source and relay are then $(1-\alpha)P_S$ and $(1-\beta)P_R$, respectively. The objective of power allocation is to determine the optimal choices of (α, β) leading to a maximal secrecy rate.

III. Power Allocation

In the first phase of DF, the source transmits $x_S = \sqrt{\alpha P_S}\, s + \sqrt{(1-\alpha)P_S}\, z$, where s is the message signal and z is the jamming signal both with unit-power. For the purpose of achieving the secrecy rate, we assume that the codewords used at the source are Gaussian inputs.

The received signal at the relay is

$$y_R = \sqrt{\alpha P_S}\, h_{S,R}\, s + \sqrt{(1-\alpha)P_S}\, h_{S,R}\, z + n_R \tag{2}$$

where n_R is the noise at the relay and follows $n_R \sim \mathcal{CN}(0, \sigma^2)$. The relay completely removes the jamming signal (i.e., the term $\sqrt{(1-\alpha)P_S}\, h_{S,R}\, z$), decodes the message signal, and re-encodes it.

For notational convenience, let us define $\gamma_{i,j} = P_i |h_{i,j}|^2/\sigma^2$ where $i \in \{S, R\}$ and $j \in \{R, D, E\}$. The rate at the relay is then given by

$$R_R = \log\left(1 + \alpha\gamma_{S,R}\right) \ . \tag{3}$$

Note that $\log(\cdot)$ denotes the base-2 logarithm throughout this paper.

In the second phase, the relay transmits $x_R = \sqrt{\beta P_R}\, s' + \sqrt{(1-\beta)P_R}\, z'$, where s' is the re-encoded message signal and z' is a new jamming signal independent of z. After removing the jamming signal at the destination, the rate at the destination is represented as

$$R_D = \frac{1}{2}\log\left(1 + \beta\gamma_{R,D}\right) \tag{4}$$

The scalar factor $1/2$ is inserted due to the fact that two channel uses are required in two phases.

We assume that the relay uses different codewords independent of the source codewords in the second phase. Then, the accumulated rate at the eavesdropper is

$$\begin{aligned} R_E \;&=\; \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_{S,E}}{1+(1-\alpha)\gamma_{S,E}}\right) \\ &\quad + \frac{1}{2}\log\left(1 + \frac{\beta\gamma_{R,E}}{1+(1-\beta)\gamma_{R,E}}\right) \ . \end{aligned} \tag{5}$$

The achievable secrecy rate can be easily calculated as

$$\begin{aligned} R_{sec} \;&=\; \frac{1}{2}\log\left[1 + (1-\alpha)\gamma_{S,E}\right] \\ &\quad + \frac{1}{2}\log\left[(1+\beta\gamma_{R,D})(1+(1-\beta)\gamma_{R,E})\right] \\ &\quad - \frac{1}{2}\log\left[(1+\gamma_{S,E})(1+\gamma_{R,E})\right] \ . \end{aligned} \tag{6}$$

Notice that the first term in Equation (6) is related to parameter α while the second term is related to β. However, α and β are not independent. The relay can correctly decode the source message if the rate at the relay is no less than the rate at the destination. In order to have successful decoding at the relay, the following condition needs to be satisfied: $\log(1+\alpha\gamma_{S,R}) \geq \log\left(1+\beta\gamma_{R,D}\right)$, which yields

$$\alpha \geq \frac{\gamma_{R,D}\beta}{\gamma_{S,R}} \ . \tag{7}$$

The secrecy rate is maximized with respect to α when Constraint (7) is active, i.e., equality holds. Substituting $\alpha = \gamma_{R,D}\beta/\gamma_{S,R}$ into Equation (6), one can see that the derivative of $4^{R_{sec}}$ with respect to β is a quadratic function in the following form.

$$\frac{\partial\, 4^{R_{sec}}}{\partial\, \beta} \quad \propto \quad A\beta^2 + B\beta + C \tag{8}$$

where

$$\begin{aligned} A &= 3\gamma_{R,D}^2\gamma_{R,E}\gamma_{S,E} \ , \\ B &= -2\gamma_{R,D}\gamma_{R,E}\gamma_{S,R}(1+\gamma_{S,E}) \\ &\quad -2\gamma_{R,D}\gamma_{S,E}[\gamma_{R,D}(1+\gamma_{R,E}) - \gamma_{R,E}] \ , \\ C &= \gamma_{S,R}(1+\gamma_{S,E})[\gamma_{R,D}(1+\gamma_{R,E}) - \gamma_{R,E}] \\ &\quad -\gamma_{R,D}\gamma_{S,E}(1+\gamma_{R,E}) \ . \end{aligned} \tag{9}$$

When the quadratic function in (8) has real root(s) (i.e., $B^2 \geq 4AC$) and the root $\frac{-B-\sqrt{B^2-4AC}}{2A}$ is within the range of $[0,1]$, β shall be selected as $\hat{\beta} = \frac{-B-\sqrt{B^2-4AC}}{2A}$. Otherwise, β shall be selected as $\hat{\beta} = 1$ representing a non-jamming scenario or $\hat{\beta} = 0$ indicating that a positive secrecy rate cannot be achieved. Note that $\hat{\beta} = \frac{-B+\sqrt{B^2-4AC}}{2A}$ is not a feasible solution as it corresponds to a minimum secrecy rate.

If $\hat{\beta} \leq \gamma_{S,R}/\gamma_{R,D}$, α shall be selected as $\hat{\alpha} = \frac{\gamma_{R,D}\hat{\beta}}{\gamma_{S,R}}$. Otherwise, if $\hat{\beta} > \gamma_{S,R}/\gamma_{R,D}$, α shall be selected as $\hat{\alpha} = 1$. In the latter case, the relay needs to reduce its transmit power to meet Constraint (7), i.e., β reduces to $\gamma_{S,R}/\gamma_{R,D}$.

The optimal power allocation is summarized as follows:

$$\begin{cases} \left(\gamma_{R,D}\hat{\beta}/\gamma_{S,R}, \hat{\beta}\right), & \text{if } \hat{\beta} \leq \gamma_{S,R}/\gamma_{R,D} \\ (1, \gamma_{S,R}/\gamma_{R,D}), & \text{elsewhere} \end{cases} \tag{10}$$

Note that a positive secrecy rate is not guaranteed even under the optimal power allocation. Substituting (10) into (6), one can compute the secrecy rate and determine whether a positive rate can be achieved.

Remarks:

- From (9), the optimal power allocation depends on the global channel knowledge. In practice, the relay may collect the global channel state information (CSI), compute the optimal power allocation, and then send the value of α to the source over a secure control channel. Recall that channel state changes are trackable due to the quasi-static assumption. In practice, the results of power allocation shall be updated periodically based on how fast the channel states change.
- In some practical scenarios, instantaneous eavesdropper's channels, i.e., $h_{S,E}$ and $h_{R,E}$, are not available, but channel statistics are available. An example is the scenario of fast fading channels for which tracking instantaneous

channel state changes may be difficult. In such scenarios, the ergodic secrecy rate is sometimes of interest. By using Jensen's inequality, the ergodic secrecy rate is upper bounded by

$$\begin{aligned}\mathbb{E}\{R_{sec}\} \quad \leq \quad & \frac{1}{2}\log\left[1+(1-\alpha)\bar{\gamma}_{S,E}\right] \\ & +\frac{1}{2}\log\left[(1+\beta\gamma_{R,D})(1+(1-\beta)\bar{\gamma}_{R,E})\right] \\ & -\frac{1}{2}\mathbb{E}\left\{\log\left[(1+\gamma_{S,E})(1+\gamma_{R,E})\right]\right\} \quad (11)\end{aligned}$$

where $\bar{\gamma}_{i,j} \triangleq P_i\mathbb{E}\{|h_{i,j}|^2\}/\sigma^2$. Power allocation for maximizing the upper bound of the ergodic rate is still specified using the result of (10). The only difference is that one has to replace $\gamma_{S,E}$ and $\gamma_{R,E}$ with $\bar{\gamma}_{S,E}$ and $\bar{\gamma}_{R,E}$, respectively. Power allocation results need not be updated unless channel statistics are changed.

- Traditional cooperative jamming schemes typically require additional costs and/or are only applicable to limited scenarios. Introducing an extra jammer requires additional hardware costs and the coordination between jammer and source is implemented with an additional overhead. When the destination has no knowledge of jamming signals, a jammer can cause interference to the destination and hence cooperative jamming is beneficial only under certain channel and power conditions [4]. Our proposed jamming strategy does not need an extra jammer and is always beneficial. However, the price we have to pay is that the legitimate receivers have the knowledge of jamming signals which can be implemented in practice with a small amount of overhead.

A. Sub-Optimal Power Allocation

As shown before, optimal power allocation depends on the global CSI, including that of the eavesdropper's channels. However, the eavesdropper's channel or even the statistics of the channel may be unavailable in practice. In this subsection, we propose two simple yet sub-optimal solutions for power allocation that do not rely on eavesdropper's channels at all.

Sub-Optimal Solution 1: From (5) and (6), if we omit the white thermal noise at the eavesdropper, it is easy to see that the secrecy rate is upper bounded by

$$R_{sec} < \frac{1}{2}\log\left((1+\beta\gamma_{RD})(1-\alpha)(1-\beta)\right) \ . \qquad (12)$$

Note that this upper bound is tight if $\gamma_{S,E} \gg 1$ and $\gamma_{R,E} \gg 1$. Now, we tend to maximize the upper bound in (12). The parameters A, B, and C in (9) can be simplified to $A = 3\gamma_{R,D}^2$, $B = -2\gamma_{R,D}\gamma_{S,R} - 2\gamma_{R,D}(\gamma_{R,D}-1)$, and $C = \gamma_{S,R}(\gamma_{R,D}-1) - \gamma_{R,D}$ which are independent of the eavesdropper's channels, i.e., $\gamma_{S,E}$ and $\gamma_{R,E}$. Other procedures remain the same as in those leading to the specification of the optimal power allocation. Furthermore, it can be readily shown that the values of α and β for this sub-optimal solution are always no greater than those in the optimal solution.

Sub-Optimal Solution 2: We assume that α is independent of β in Equation (6), and as such only the second term in Equation (6) is related to β. Taking the derivative of the second term in (6) and setting it to zero, we can easily find the solution for β as:

$$\hat{\beta} \quad = \quad \frac{1}{2} + \frac{\gamma_{R,E}^{-1} - \gamma_{R,D}^{-1}}{2} \approx \frac{1}{2} - \frac{\gamma_{R,D}^{-1}}{2} \ . \qquad (13)$$

In the above, we have assumed that $\gamma_{R,E} >> 1$. The power allocation corresponds to (10) in which $\hat{\beta}$ is given by (13). In scenarios of interest, the $R \rightarrow E$ link may not be too weak or else the effects of the eavesdropper are trivial. Hence, the assumption of $\gamma_{R,E} \gg 1$ is usually satisfied.

B. Two Benchmark Schemes

In this subsection, we analyze the power allocation problems of two benchmark schemes, for the purpose of performance comparisons used in Section IV.

Benchmark 1: For the first benchmark, we consider a traditional DF-based relaying scheme without taking into account the presence of the eavesdropper. Again, we denote αP_S to be the source's power for transmitting its message and βP_R to be the relay's power for transmitting its message. Consequently, only Constraint (7) needs to be satisfied. If $\gamma_{S,R} \neq \gamma_{R,D}$, the source or relay need not use all of its available power. The power allocation is given by (10) where $\hat{\beta} = 1$.

Benchmark 2: For the second benchmark, we consider a DF-based relaying scheme without jamming while taking into account the presence of the eavesdropper. For this case, the source or relay does not transmit any jamming signal but may not use all of its available power. In this case, Constraint (7) needs to be satisfied and the secrecy rate is identified as

$$R_{sec} = \frac{1}{2}\log\left(\frac{1+\beta\gamma_{R,D}}{1+\beta\gamma_{R,E}}\right) - \frac{1}{2}\log\left(1+\alpha\gamma_{S,E}\right) \qquad (14)$$

Substituting $\alpha = \gamma_{R,D}\beta/\gamma_{S,R}$ into (14), we further derive

$$4^{R_{sec}} = \frac{1+\beta\gamma_{R,D}}{(1+\beta\gamma_{R,E})(1+\gamma_{R,D}\gamma_{S,E}\beta/\gamma_{S,R})} \ . \qquad (15)$$

Taking the derivative of $4^{R_{sec}}$ with respect to β, we obtain

$$\begin{aligned}\frac{\partial\ 4^{R_{sec}}}{\partial\ \beta} \quad \propto \quad & (\gamma_{S,R}/\gamma_{S,E}-1)(\gamma_{R,D}/\gamma_{R,E}-1) \\ & -(\gamma_{R.D}\beta+1)^2 \qquad (16)\end{aligned}$$

The optimal value of β is 0, 1, or $\frac{1}{\gamma_{R,D}}\left[\sqrt{(\gamma_{S,R}/\gamma_{S,E}-1)(\gamma_{R,D}/\gamma_{R,E}-1)}-1\right]$.

Remark: As compared to the second benchmark scheme, the secrecy rate for the proposed jamming scheme could not be improved, if the relay and destination do not have the knowledge of jamming signals. The proof is provided in the Appendix.

IV. Numerical Results

In this section, we investigate the performance of the proposed power allocation results via numerical experiments. Channels between any two nodes are modeled using frequency non-selective Rayleigh fading with a path loss, i.e., $h_{i,j} \sim$

$\mathcal{CN}(0, d_{i,j}^{-c})$ where $d_{i,j}$ is the distance between node i and node j, and $c = 4$ is the path loss exponent. For simplicity, we consider a simple one-dimensional system model as illustrated in Fig. 2 in which source, relay, destination, and eavesdropper are placed along a horizontal line. The locations of source, relay, and destination are fixed at coordinates $(-1, 0)$, $(0, 0)$, and $(1, 0)$, respectively. The average signal-to-noise ratio (SNR) of the $S \rightarrow R$ and $R \rightarrow D$ links, i.e., $\bar{\gamma}_{S,R}$ and $\bar{\gamma}_{R,D}$ are fixed at 15 dB. We perform Monte-Carlo experiments consisting of 10^5 independent trials with independent channel realizations to obtain average results.

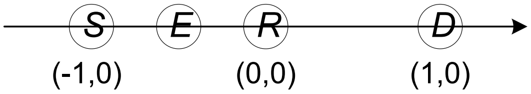

Fig. 2. An illustration of the simulation model.

In Fig. 3, we show the average secrecy rates of DF-based relaying versus the eavesdropper's locations under various power allocation solutions. In our numerical experiments, we move the eavesdropper's location from $(-4, 0)$ to $(3, 0)$ to evaluate the secrecy rate. The power allocation solutions in Fig 3 include the optimal power allocation proposed by Equation (10), the two sub-optimal power allocation solutions proposed in Section III-A, and the two benchmarks proposed in Section III-B. As expected, the optimal power allocation always outperforms the two sub-optimal solutions and the two benchmarks. As for the two sub-optimal solutions, it appears that the first one is a better solution when the eavesdropper is close to the source and relay, while the second one is a better solution when the eavesdropper is far away from the source and relay. Since the second benchmark takes into account the presence of the eavesdropper, it performs slightly better than the first benchmark. As observed, when the eavesdropper moves close to the source and relay, the secrecy rate for all curves decreases since $\gamma_{S,E}$ and $\gamma_{R,E}$ increase and the eavesdropper plays an increasingly significant role. A positive secrecy rate could be always achieved for the proposed jamming strategy, while for traditional DF-relaying without jamming a positive secrecy rate could be achieved only if the eavesdropper is far away from the source and relay. For the proposed jamming strategy, the minimal secrecy rate occurs when the eavesdropper is located approximately in the middle of source and relay, i.e., the coordinates $(-0.5, 0)$. This is because at this location both the $S \rightarrow E$ link and the $R \rightarrow E$ link are strong.

In Fig. 4, we further show the average values of parameters α and β for the same simulation scenario as in Fig. 3. As observed, the power allocations of the two sub-optimal schemes are independent of the eavesdropper's locations, since no eavesdropper's channels are needed (see the discussion of Section III-A). In addition, the parameter values of Sub-optimal Solution 1 is no greater than those of the optimal power allocation, which is in agreement with the conclusion in Section III-A.

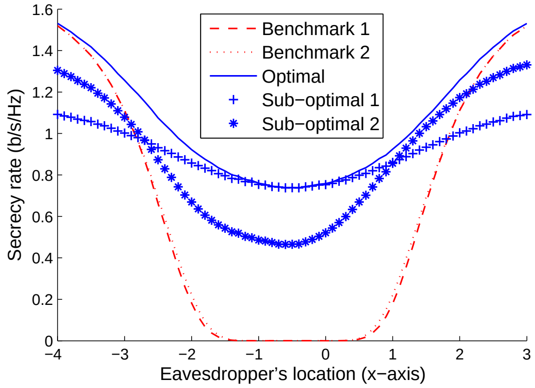

Fig. 3. The secrecy rates under different power allocation schemes.

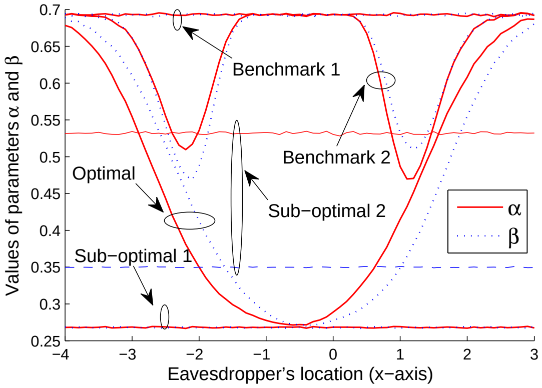

Fig. 4. The parameter values under different power allocation schemes.

V. Conclusions and Future Work

In this paper, we proposed a jamming scheme capable of improving the physical layer security of a two-hop decode-and-forward wireless relay network in the presence of an eavesdropper. In addition to transmitting message signals, we allowed the source and relay to allocate some of their available power for transmitting jamming signals in order to interfere with the eavesdropper. We formulated and solved a constrained optimization problem aiming at allocating transmission powers associated with message and jamming signals such that the achievable secrecy rate subject to power constraints on the source and on the relay is maximized. We showed that the optimal power allocation depends on the global channel state information. Furthermore, we proposed two simple yet sub-optimal power allocation schemes that did not rely on eavesdropper's channels. We also analyzed power allocation problems for two benchmark schemes without jamming. Numerical results confirmed that our proposed jamming scheme could significantly improve the secrecy rate. Further work includes the analysis of power allocation problems for other scenarios of interest such as AF-based relaying.

Appendix

In this section, we show that, if legitimate receivers do not have the knowledge of jamming signals, the secrecy rate of the proposed jamming strategy is no more than that of traditional DF-relaying without jamming.

Without jamming knowledge at legitimate receivers, the secrecy rate of the proposed jamming strategy can be easily calculated as

$$\begin{aligned} R_{sec} &= \frac{1}{2}\log\left[1+(1-\alpha)\gamma_{S,E}\right]+\frac{1}{2}\log\left(\frac{1+(1-\beta)\gamma_{R,E}}{1+(1-\beta)\gamma_{R,D}}\right) \\ &\quad +\frac{1}{2}\log\left(\frac{1+\gamma_{R,D}}{(1+\gamma_{S,E})(1+\gamma_{R,E})}\right) . \end{aligned} \tag{17}$$

It is also clear that if $\gamma_{S,R} \leq \gamma_{S,E}$ or $\gamma_{R,D} \leq \gamma_{R,E}$, it would be impossible to achieve a positive secrecy rate. Therefore, in what follows we only focus on the cases of $\gamma_{S,D} > \gamma_{S,E}$ and $\gamma_{R,D} > \gamma_{R,E}$.

For DF-relaying without jamming, we assume that the presence of the eavesdropper is a priori, so the source and relay may not use all of their available power.

Proposition 1: For an arbitrary $\beta \in [0,1]$, we consider the following two cases for Phase 2:

Case 1) The relay's power $(1-\beta)P_R$ is used for transmitting a jamming signal.

Case 2) The relay's power $(1-\beta)P_R$ is used for transmitting neither the message nor the jamming signal.

Other conditions or parameters are the same for both cases.

Then, the secrecy rate in case 1) is always no more than that in case 2).

Proof: For convenience, let us denote the secrecy rate in case 1) by $R_{sec}^{(1)}$ and the secrecy rate in case 2) by $R_{sec}^{(2)}$, respectively.

$$\begin{aligned} R_{sec}^{(1)} - R_{sec}^{(2)} &= \log\left(\frac{(1+\gamma_{R,D})[1+(1-\beta)\gamma_{R,E}]}{(1+\gamma_{R,E})[1+(1-\beta)\gamma_{R,D}]}\right) \\ &\quad -\log\left(\frac{1+\beta\gamma_{R,D}}{1+\beta\gamma_{R,E}}\right) \\ &= \log\left(1+\frac{(\gamma_{R,D}-\gamma_{R,E})\beta}{(1+\gamma_{R,E})[1+(1-\beta)\gamma_{R,D}]}\right) \\ &\quad -\log\left(1+\frac{(\gamma_{R,D}-\gamma_{R,E})\beta}{1+\beta\gamma_{R,E}}\right) \\ &\leq 0 \end{aligned} \tag{18}$$

■

Similarly, one can show that the same conclusion as in Propositions 1 is also valid for Phase 1. Thus, it follows that the secrecy rate of the proposed jamming strategy cannot be enhanced if the legitimate receivers do not have an apriori knowledge of jamming signals.

References

[1] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security.* Now Publishers, Delft, The Netherlands, 2009.

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

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

[4] R. Liu and W. Trappe (Ed.), *Securing Wireless Communications at the Physical Layer.* Springer, 2010.

[5] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062 - 3080, Dec. 2004.

[6] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity - Part I: System description," *IEEE Trans. Commun.*, vol. 51, no.11, pp.1927 - 1938, Nov. 2003.

[7] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation in diversity - Part II: Implementation aspects and performance analysis," *IEEE Trans. Commun.*, vol. 51, pp. 1939-1948, Nov. 2003.

[8] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005 - 4019, Sept. 2008.

[9] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, " Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 494696, 14 pages, 2009.

[10] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wiretapper," in *Proc. 2007 IEEE Information Theory Workshop*, Lake Tahoe, CA, Sept. 2007.

[11] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming." in *Proc. 2008 IEEE Global Telecommunications Conference*, New Orleans, LA, Nov. - Dec. 2008.

[12] R. Negi and S. Goelm, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Tech. Conf*, vol. 3, Dallas TX, pp. 1906-1910, Sept. 2005.

[13] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Sig. Proc.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[14] J. Zhang, M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. the IEEE International Conference on Communication (ICC)*, Cape Town, South Africa, May 2010.