Decode-and-Forward Relay Beamforming with Secret and Non-Secret Messages

Sanjay Vishwakarma and A. Chockalingam
Email: sanjay@ece.isc.ernet.in, achockal@ece.isc.ernet.in
Department of ECE, Indian Institute of Science, Bangalore 560012

Abstract—In this paper, we study beamforming in decode-and-forward (DF) relaying using multiple relays, where the source node sends a secret message as well as a non-secret message to the destination node in the presence of multiple non-colluding eavesdroppers. The non-secret message is transmitted at a fixed rate $R_0$, and requires no protection from the eavesdroppers, whereas the secret message needs to be protected from the eavesdroppers. The source and relays operate under a total power constraint. We find the optimum source powers and weights of the relays for both secret and non-secret messages which maximize the worst case secrecy rate for the secret message as well as meet the information rate constraint $R_0$ for the non-secret message. We solve this problem for two cases of channel state information (CSI) assumption. In the first case, perfect CSI of all links is assumed. In the second case, only the statistical CSI of the eavesdroppers links and perfect CSI of other links are assumed to be known.

Notations: $A \in \mathbb{C}^{N_1 \times N_2}$ implies that $A$ is a complex matrix of dimension $N_1 \times N_2$, $A \succeq 0$ denotes that $A$ is a positive semidefinite matrix. Transpose and complex conjugate transpose operations are denoted by $[\cdot]^T$ and $[\cdot]^*$, respectively. $\| \cdot \|$ denotes 2-norm operation. $\mathbb{E} [\cdot]$ denotes the expectation operator.

II. System Model

Consider a DF cooperative relaying scheme which consists of a source node $S$, $N$ relay nodes $\{r_1, r_2, \cdots, r_N\}$, an intended destination node $D$, and $J$ non-colluding eavesdropper nodes $\{e_1, e_2, \cdots, e_J\}$. The system model is shown in Fig. 1. In addition to the links from relays to destination node and relays to eavesdropper nodes, we assume direct links from source to destination node and source to eavesdropper nodes. The complex fading channel gains between the source to relays are denoted by $\gamma = [\gamma_1, \gamma_2, \cdots, \gamma_N] \in \mathbb{C}^{1 \times N}$. Likewise, the channel gains between the relays to destination and the relays to $j$th eavesdropper are denoted by $\alpha = [\alpha_1, \alpha_2, \cdots, \alpha_N] \in \mathbb{C}^{1 \times N}$ and $\beta_{j} = [\beta_{1j}, \beta_{2j}, \cdots, \beta_{Nj}] \in \mathbb{C}^{1 \times N}$, respectively, where $j = 1, 2, \cdots, J$. The channel gains on the direct links from the source to destination and the source to $j$th eavesdropper are denoted by $\alpha_{0}$ and $\beta_{0j}$, respectively.

Let $P_T$ denote the total transmit power budget in the system (i.e., source power plus relays power). The communication between source $S$ and destination $D$ happens in two hops. Each hop is divided into $n$ channel uses. In the first hop of transmission, the source $S$ transmits two independent messages $W_0$ and $W_1$ which are equiprobable over $\{1, 2, \cdots, 2^{2nR_0}\}$ and $\{1, 2, \cdots, 2^{2nR_s}\}$, respectively. $W_0$ is the non-secret message to be conveyed to the destination at a fixed information rate $R_0$ which need not be protected from $E_2$. $W_1$ is the secret message which has to be conveyed to the destination at some rate $R_s$ with perfect secrecy [7], i.e., $W_1$ needs to be protected from all $E_2$'s. For each $W_0$ drawn equiprobably from the set $\{1, 2, \cdots, 2^{2nR_0}\}$, the source $S$ maps $W_0$ to...
Fig. 1. DF relay beamforming with secret and non-secret messages.

an iid ($\sim \mathcal{CN}(0, 1)$) codeword $X^0_1, X^0_2, \ldots, X^0_n$ of length $n$. Similarly, for each $W_i$ drawn equiprobably from the set \{1, 2, \ldots, $2^nR_i$\}, the source $S$, using a stochastic encoder, maps $W_i$ to an iid ($\sim \mathcal{CN}(0, 1)$) codeword $X^1_1, X^1_2, \ldots, X^1_n$ of length $n$. Let $P^0_s$ and $P^1_s$ denote the source transmit powers corresponding to the codewords $X^0_1, X^0_2, \ldots, X^0_n$ and $X^1_1, X^1_2, \ldots, X^1_n$, respectively. In the $k$th ($1 \leq k \leq n$) channel use, the source transmits the sum of the weighted symbols, i.e., $\sqrt{P^0_s}X^0_k + \sqrt{P^1_s}X^1_k$. In the following, we will use $X^0$ and $X^1$ to denote the symbols in the codewords $X^0_1, X^0_2, \ldots, X^0_n$ and $X^1_1, X^1_2, \ldots, X^1_n$, respectively.

In the second hop of transmission, relays retransmit the decoded symbols $X^0$ and $X^1$ to the destination $D$. Let $\phi = [\phi_1, \phi_2, \ldots, \phi_N]^T \in \mathbb{C}^{N \times 1}$ and $\psi = [\psi_1, \psi_2, \ldots, \psi_N]^T \in \mathbb{C}^{N \times 1}$ denote the complex weights applied by the relays corresponding to the transmit symbols $X^0$ and $X^1$, respectively. The $i$th ($1 \leq i \leq N$) relay transmits the sum of the weighted symbols which is $\phi_i X^0 + \psi_i X^1$.

Let $y_{R_i}$, $y_{D_i}$, and $y_{E_{ij}}$ denote the received signals at the $i$th relay, destination $D$, and $j$th eavesdropper $E_j$, respectively, in the first hop of transmission. In the second hop of transmission, the received signals at the destination and $j$th eavesdropper are denoted by $y_{D_2}$ and $y_{E_{2j}}$, respectively. We then have

\[
y_{R_i} = \sqrt{P^0_s} \gamma_i X^0 + \sqrt{P^1_s} \gamma_i X^1 + \eta_{R_i}, \quad \forall i = 1, 2, \ldots, N, \quad (1)
\]
\[
y_{D_i} = \sqrt{P^0_s} \alpha_0 X^0 + \sqrt{P^1_s} \alpha_0 X^1 + \eta_{D_i}, \quad (2)
\]
\[
y_{E_{1j}} = \sqrt{P^0_s} \beta_{ij} X^0 + \sqrt{P^1_s} \beta_{ij} X^1 + \eta_{E_{1j}}, \quad \forall j = 1, 2, \ldots, J, \quad (3)
\]
\[
y_{D_2} = \alpha \phi X^0 + \alpha \psi X^1 + \eta_{D_2}, \quad (4)
\]
\[
y_{E_{2j}} = \beta_j \phi X^0 + \beta_j \psi X^1 + \eta_{E_{2j}}, \quad \forall j = 1, 2, \ldots, J. \quad (5)
\]

The noise components, $\eta$’s, are assumed to be iid $\mathcal{CN}(0, N_0)$.

III. BEAMFORMING WITH SECRET AND NON-SECRET MESSAGES - KNOWN CSI ON ALL LINKS

In this section, we assume perfect knowledge of the CSI on all links. This assumption can be valid in scenarios where the eavesdopers are also legitimate users in the network. Since the symbol $X^0$ is transmitted at information rate $R_0$ irrespective of $X^1$, treating $X^1$ as noise, relays will be able to decode $X^0$ if $\forall i = 1, 2, \ldots, N$,

\[
\frac{1}{2} I(\gamma_i; y_{R_i}) = \frac{1}{2} \log_2 \left( 1 + \frac{P^0_s | \gamma_i |^2}{N_0 + P^1_s | \gamma_i |^2} \right) \geq R_0, \quad (6)
\]

where (6) is derived using (1) and the factor 1/2 appears because of the two hops. Similarly, using (2) and (4), the destination $D$ will be able to decode $X^0$ if

\[
\frac{1}{2} I(\gamma_i; y_{D_1}, y_{D_2}) = \frac{1}{2} \log_2 \left( 1 + \frac{P^0_s | \alpha_0 |^2}{N_0 + P^1_s | \alpha_0 |^2} + \frac{\phi^* \phi + \psi^* \psi}{N_0} \right) \geq R_0. \quad (7)
\]

Using (1) and with the knowledge of the symbol $X^0$, the information rate for $X^1$ at the $i$th relay is

\[
\frac{1}{2} I(\gamma_i; y_{R_i}; X^0) = \frac{1}{2} \log_2 \left( 1 + \frac{P^1_s | \gamma_i |^2}{N_0} \right). \quad (8)
\]

Similarly, using (2) and (3), the information rate for $X^1$ at the destination $D$ is

\[
\frac{1}{2} I(\gamma_i; y_{D_1}, y_{D_2}) = \frac{1}{2} \log_2 \left( 1 + \frac{P^1_s | \alpha_0 |^2}{N_0} + \frac{\psi^* \beta_j \beta_j^* \psi}{N_0} \right). \quad (9)
\]

Using (3), (5), and assuming the knowledge of $X^0$ at the eavesdroppers, the information rate for $X^1$ at eavesdropper $E_j$ is

\[
\frac{1}{2} I(\gamma_i; y_{E_{1j}}, y_{E_{2j}}; X^0) = \frac{1}{2} \log_2 \left( 1 + \frac{P^1_s | \beta_{ij} |^2}{N_0} + \frac{\psi^* \beta_j \beta_j^* \psi}{N_0} \right). \quad (10)
\]

We note that there is no decoding constraint for the symbol $X^0$ on any eavesdropper $E_j$ similar to (6) and (7). This makes (10) as the best possible information rate for symbol $X^1$ at $E_j$. Further, with the knowledge of symbol $X^0$, the relays will be able to decode the symbol $X^1$ if $\forall i = 1, 2, \ldots, N$.

\[
\frac{1}{2} I(\gamma_i; y_{R_i}; X^0) \geq \frac{1}{2} I(\gamma_i; y_{R_i}; X^0), \quad (11)
\]

i.e.,

\[
\frac{1}{2} \log_2 \left( 1 + \frac{P^1_s | \gamma_i |^2}{N_0} \right) \geq \frac{1}{2} \log_2 \left( 1 + \frac{P^1_s | \gamma_i |^2}{N_0} + \frac{\psi^* \beta_j \beta_j^* \psi}{N_0} \right). \quad (12)
\]

The constraint on the total transmit power is

\[
P^0_s + P^1_s + \phi^* \phi + \psi^* \psi \leq P_T. \quad (13)
\]
Subject to the constraints in (6), (7), (12), and (13), the worst case achievable secrecy rate for $X^1$ is obtained by solving the following optimization problem [12][15]:

$$R_s = \max_{\phi, \psi} \min_{j:1,2,\ldots,J} \left\{ \frac{1}{2} I(X^1; y_{D_1}, y_{D_2}|X^0) - \frac{1}{2} I(X^1; y_{E_1}, y_{E_2}|X^0) \right\}^+, \quad \text{s.t.}$$

$$\frac{1}{2} I(X^0; y_{R_i}) \geq R_0, \quad \forall i = 1, 2, \ldots, N, \quad (15)$$

$$\frac{1}{2} I(X^0; y_{D_1}, y_{D_2}) \geq R_0, \quad (16)$$

$$\frac{1}{2} I(X^1; y_{R_i}|X^0) \geq \frac{1}{2} I(X^1; y_{D_1}, y_{D_2}|X^0), \quad \forall i = 1, 2, \ldots, N, \quad (17)$$

where $\{a\}^+ = \max(a, 0)$, and without loss of generality we drop this operator since secrecy rate is non-negative. The constraints (15), (16), and (17) are obtained from (6), (7), and (12), respectively. The objective function in (14) is obtained from (9) and (10). We solve the optimization problem in (14) as follows.

**Step1**: Divide the total available transmit power $P_T$ in $M$ discrete steps of size $\Delta P_m = \frac{P_T}{M}$, and let $P_m = m \Delta P_m$, where $m = 0, 1, 2, \ldots, M - 1$.

**Step2**: Rewrite the optimization problem (14) as the following two separate optimization problems; Problem 1 and Problem 2.

**Problem 1:**

$$\max_{P_s^0, \phi, \psi} \min_{j:1,2,\ldots,J} \frac{1}{2} \left[ \log_2 \left( 1 + \frac{P_s^0 | \alpha_0 |^2 + \psi^* \phi \psi^* \phi^*}{N_0} \right) \right]$$

$$- \log_2 \left( 1 + \frac{P_s^1 | \beta_0 |^2 + \psi^* \beta_j^* \psi^*}{N_0} \right), \quad (19)$$

s.t.

$$\forall i = 1, 2, \ldots, N, \quad \frac{1}{2} \log_2 \left( 1 + \frac{P_s^0 | \gamma_i |^2}{N_0} \right) \geq 0, \quad \left(1 + \frac{P_s^1 | \alpha_0 |^2 + \psi^* \alpha \alpha^* \alpha^*}{N_0} \right), \quad P_s^0 \geq 0, \quad P_s^1 + \psi^* \psi \leq P_m. \quad (20)$$

The optimization problem in (19) is a function of $P_s^1$, $\psi$, and $P_m$. For a given $P_m$, it can be solved using semi-definite relaxation technique in [15].

**Problem 2:**

$$\min_{\phi, \psi, s.t.} \forall i = 1, 2, \ldots, N,$$

$$\frac{1}{2} \log_2 \left( 1 + \frac{P_s^0 | \gamma_i |^2}{N_0} \right) \geq R_0,$$

$$\frac{1}{2} \log_2 \left( 1 + \frac{P_s^0 | \alpha_0 |^2 + \phi^* \alpha \alpha^* \alpha^*}{N_0} \right) \geq R_0,$$

$$P_s^0 \geq 0, \quad P_s^0 + \phi^* \phi \leq P_T - P_m. \quad (22)$$

For a given $P_s^1$, $\psi$, and $P_m$, it is obvious that the optimum direction of $\phi$ which minimizes the transmit power $P_s^0 + \phi^* \phi$, subject to the constraints in (22), lies in the direction of $\alpha^*$, i.e., $\phi = \sqrt{P_s^0} \phi_u$, where $\phi_u = \frac{\alpha^*}{|\alpha^*|}$ and $P_s^0$ is the relays transmit power associated with $X_0$.

**Problem 3:**

$$\min_{\phi, \psi}\text{s.t.}$$

$$\left(1 + \frac{P_s^0 | \alpha_0 |^2 + \psi^* \phi \psi^* \phi^*}{N_0} \right) \geq 2 R_0, \quad \forall i = 1, 2, \ldots, N,$$

$$\left(1 + \frac{P_s^0 | \alpha_0 |^2 + \psi^* \phi \psi^* \phi^*}{N_0} \right) \geq 2 R_0,$$

$$P_s^0 \geq 0, \quad P_r^0 \geq 0, \quad P_s^0 + P_r^0 \leq P_T - P_m. \quad (24)$$

For a given $P_s^1$, $\psi$, and $P_m$, the feasibility problem in (24) with its constraints in (24) is a linear feasibility problem in $P_s^0$ and $P_r^0$, and it can be easily solved using linear programming techniques.

It can be shown that the secrecy rate $R_m$ which is obtained by solving the optimization problem (19) for a given $P_m$ is a strictly increasing function in $P_m$ [15]. Hence, the idea is to find the maximum power $P_m$ for which $P_s^1$ and $\psi$ obtained by solving (19) also gives a feasible solution $P_s^0$ and $P_r^0$ in (24) satisfying the constraints in (24). This can be achieved by decreasing $m$ from $M - 1$ towards 0 and finding the maximum $m$ for which the solution of the optimization problem (19) (i.e., $P_s^1$, $\psi$) with $P_m$ as available power also gives a feasible solution for (23) (i.e., $P_s^0$ and $P_r^0$ satisfying the constraints in (24)).

**A. Suboptimal beamforming with non-secret message for D and all E_j's**

In this subsection, we give a suboptimal beamforming method with secret and non-secret messages where the secret message $W_1$ is intended only for $D$ whereas the non-secret message $W_0$ is intended for $D$ as well as all $E_j$s. The non-secret message is transmitted at a fixed rate $R_0$. Similar to (7), using (3), (5) and treating $X^1$ as noise, $E_j$s will be able to decode $X^0$ if $\forall j = 1, 2, \ldots, J$,

$$\frac{1}{2} I(X^0; y_{E_1}, y_{E_2}) = \frac{1}{2} \log_2 \left( 1 + \frac{P_s^0 | \beta_0 |^2}{N_0} + \frac{P_s^1 | \beta_0 |^2}{N_0} \right) + \frac{\phi^* \beta_j^* \beta_j \phi}{N_0 + \psi^* \beta_j^* \beta_j \psi} \geq R_0. \quad (25)$$

With this, the optimization problem in (14) will have additional constraints (25). Similarly, the feasibility problem (21) will
have the additional constraints (25). For a given $P^1_s$, $\psi$, and $P_m$, the optimum direction of $\phi$ which minimizes the transmit power $P^0_s + \phi^* \phi$, can be obtained by solving the following optimization problem:

$$\min_{P^0_s, \Phi} \quad P^0_s + \text{trace}(\Phi), \quad (26)$$

subject to:

$$\forall i = 1, 2, \cdots, N, \quad \frac{1}{2} \log_2 \left( 1 + \frac{P^1_s | \alpha_i |^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right) \geq 0,$$

$$\left( 1 + \frac{P^0_s | \alpha_0 |^2}{N_0 + P^1_s | \beta_0 |^2} \right) \frac{\alpha \Phi \alpha^*}{N_0 + \psi^* \alpha^* \alpha \psi} \geq 2^2 R_0,$$

$$\left( 1 + \frac{P^0_s | \beta_j |^2}{N_0 + P^1_s | \beta_j |^2} \right) \frac{\beta_j \Phi \beta_j^*}{N_0 + \psi^* \beta_j^* \beta_j \psi} \geq 2^2 R_0,$$

$$\forall j = 1, 2, \cdots, J, \quad \Phi \succeq 0, \quad \text{rank}(\Phi) = 1,$$

$$P^0_s \geq 0, \quad P^0_s + \text{trace}(\Phi) \leq P_T - P_m, \quad (27)$$

where $\Phi = \phi \phi^*$ and the constraints in (27) are written using all the constraints in (22) and (25). This is a non-convex optimization problem which is difficult to solve. However, by relaxing the $\text{rank}(\Phi) = 1$ constraint, the above problem can be solved using semi-definite programming techniques. But, the solution of the above rank relaxed optimization problem may not have rank 1. So, we take the largest eigen direction of $\Phi$ as the suboptimal unit norm direction $\phi_u$. We substitute $\phi_u$ in the feasibility problem (23) and its constraints (24) and additional constraints (28). The remaining procedure to find $P^0_s$, $P^1_s$, $P^R_s$ and $\psi$ remains same as discussed in Step1 and Step2.

IV. BEAMFORMING WITH SECRET AND NON-SECRET MESSAGES – STATISTICAL CSI ON EAVESDROPPERS LINKS

In this section, we obtain the source and relays powers under the assumption that only the statistical knowledge of the eavesdropper CSI is available. The eavesdropper CSI is assumed to be iid $CN(0, \sigma^2_{\beta_0})$ for the direct link from source to $E_j$ and iid $CN(0, \sigma^2_{\beta_{ij}})$ for the link from relay $i$ to $E_j$. With this statistical knowledge of the eavesdroppers CSI, the optimization problem (19) can be written in the following form:

$$\max_{P^1_s, \psi, j=1,2,\ldots, J} \min_{P^0_s} \frac{1}{2} \left\{ \log_2 \left( 1 + \frac{P^1_s | \alpha_0 |^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right) \right\}$$

$$- \mathbb{E} \left[ \log_2 \left( 1 + \frac{P^1_s | \beta_{0j} |^2 + \psi^* \beta_{0j}^* \beta_{0j} \psi}{N_0} \right) \right], \quad (28)$$

$$\max_{P^1_s, \psi, j=1,2,\ldots, J} \min_{P^0_s} \frac{1}{2} \left\{ \log_2 \left( 1 + \frac{P^1_s | \alpha_0 |^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right) \right\}$$

$$- \log_2 \left( 1 + \frac{P^1_s \sigma^2_{\beta_0j} + \psi^* \Lambda_j \psi}{N_0} \right), \quad (29)$$

s.t. $\forall i = 1, 2, \cdots, N, \quad \frac{1}{2} \log_2 \left( 1 + \frac{P^1_s | \gamma_i |^2}{N_0} \right) \geq 0$, $P^1_s \geq 0, \quad P^1_s + \psi^* \psi \leq P_m, \quad (30)$

where the lower bound in (29) is due to Jensen’s inequality. The $\Lambda_j$ in (29) is a diagonal matrix with $[\sigma^2_{\beta_1}, \sigma^2_{\beta_2}, \cdots, \sigma^2_{\beta_N}]^T$ on its diagonal. For a given $P_m$, the optimization problem (29) can be solved using semi-definite relaxation. The optimal $P^0_s, P^1_s, P^R_s$, and $\psi$ can be obtained by solving the optimization problems (29) and (23) as discussed in Section III.

V. RESULTS AND DISCUSSIONS

We present the numerical results and discussions in this section. We obtained the secrecy rate results through simulations for $N = 2$ relays and $J = 1, 2, 3$ eavesdroppers. The following complex channel gains are taken in the simulations: $\alpha_0 = 0.3039 + 0.5128i$, $\beta_{01} = 0.1161 - 0.0915i$, $\beta_{02} = -0.5194 + 0.4268i$, $\beta_{03} = 0.0900 + 0.4769i$, $\gamma_1 = [-1.3136 + 0.3534i, -0.7070 - 1.1305i], \alpha = [0.3241 + 0.4561i, 0.2713 - 0.5850i]$, $\beta_1 = [-0.6407 + 0.0709i, -0.0562 + 0.5120i]$, $\beta_j = [0.1422 - 0.6060i, -0.0590 - 0.3308i]$, and $\beta_3 = [0.2793 - 0.1426i, -0.5092 + 0.2570i]$. For the case of statistical CSI on eavesdroppers links, the following parameters are taken: $\sigma^2_{\beta_{01}} = 0.01, \sigma^2_{\beta_{02}} = 0.04, \sigma^2_{\beta_{03}} = 0.09, \sigma^2_{\beta_{1}} = 0.25$, $\sigma^2_{\beta_{1}} = 0.36, \sigma^2_{\beta_{1}} = 0.49, i = 1, 2$. The value of $M$ is taken to be 50.

Perfect CSI on All Links: Figure 2(a) shows the secrecy rate plots for DF relay beamforming as a function of total transmit power ($P_T$) for the case when perfect CSI on all links is assumed. The secrecy rates are plotted for the cases of with and without $W_0$ for 2 relays and different number of eavesdroppers. For the case with $W_0$, the information rate of the $W_0$ is fixed at $R_0 = 0.2$. We also assume that when $W_0$ is present, it is intended only for $D$ and it need not be protected from $E_j$s. From Fig. 2(a), we observe that, for a given number of eavesdroppers, the secrecy rate degrades when $W_0$ is present. However, this degradation becomes insignificant when $P_T$ is increased to large values. Also, the secrecy rate degrades for increasing number of eavesdroppers. Figure 2(b) shows the $R_s$ vs $R_0$ tradeoff, where $R_s$ is plotted as a function of $R_0$ for $J = 1, 2, 3$ at a fixed total power of $P_T = 6$ dB. It can be seen that as $R_0$ is increased, secrecy rate decreases. This is because the available transmit power for $W_1$ decreases as $R_0$ is increased. In Fig. 2(b), we see that the maximum achievable secrecy rate $R_s$ without $W_0$ (i.e., when $R_0 = 0$), which we denote by $R'_s$, are 0.58, 0.45 and 0.28 for $J = 1, 2, 3$ eavesdroppers, respectively. It can be further noted that if $R_0 \leq R'_s$, then $W_0$ can also be transmitted as a secret message and the remaining rate $R'_s - R_0$ can be used for the secret message ($W_1$) transmission. In other words, if $R_0 \leq R'_s$, then it is possible for both $W_1$ and $W_0$ to be sent as secret message.
at a combined secrecy rate $R_s'$. However, if $R_0 > R_s'$, then $W_0$ cannot be transmitted as a secret message.

Statistical CSI on eavesdroppers links: Figures 3(a) and (b) show the secrecy rate plots for DF relay beamforming for the case when only the statistical CSI on eavesdroppers links is assumed to be perfectly known. The CSI on other links are assumed to be perfectly known. Figure 3(a) shows the secrecy rate versus $P_T$ plots for $R_0 = 0.2$, and Fig. 3(b) shows the secrecy rate versus $R_0$ plots for $P_T = 6$ dB. Observations similar to those in the case of perfect CSI on all links are observed in Figs. 3(a) and 3(b) as well.

VI. CONCLUSIONS

We investigated beamforming in DF relaying using multiple relays, where the source sends a secret message as well as a non-secret message to the destination node in the presence of multiple non-colluding eavesdroppers. The source and relays operate under a total power constraint. We obtained the optimum source powers and weights of the relays for both secret and non-secret messages which maximized the worst case secrecy rate for the secret message as well as met the information rate constraint $R_0$ for the non-secret message. We solved this problem for the cases when (i) perfect CSI of all links was known, and (ii) only the statistical CSI of the eavesdroppers links and perfect CSI of other links were known.

REFERENCES

[1] A. Wyner, “The wire-tap channel,” Bell. Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Jan. 1975.
[2] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol. IT-24, pp. 339-348, May 1978.
[3] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channels with common and confidential messages,” IEEE Trans. Inform. Theory, vol. IT-24, pp. 451-456, Jul. 1978.
[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Information theoretic security,” Foundations and Trends in Communications and Information Theory, NOW Publishers, vol. 5, no. 4-5, 2009.
[5] A. Khisti and G. Wornell, “Secure transmission with multiple antennas-I: The MISO/MIMO wiretap channel,” IEEE Trans. Inform. Theory, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.
[6] A. Khisti and G. Wornell, “Secure transmission with multiple antennas-II: The MIMOME wiretap channel,” IEEE Trans. Inform. Theory, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.
[7] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wiretap channels,” EURASIP Journ. on Wireless Commun. and Net., vol. 2009, article ID 142374, 12 pages. doi:10.1155/2009/142374
[8] H. D. Ly, T. Liu, and Y. Liang, “Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages,” IEEE Trans. Inform. Theory, vol. 56, no. 11, pp. 5477-5487, Nov. 2010.
[9] E. Ekrem and S. Ulukus, “Capacity region of Gaussian MIMO broadcast channels with common and confidential messages,” IEEE Trans. Inform. Theory, vol. 58, no. 9, pp. 5669-5680, Sep. 2012.
[10] R. Liu, T. Liu, and H. V. Poor, “New results on multiple-input multiple-output broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol. 59, no. 3, pp. 1346-1359, Mar. 2013.
[11] L. Lai and H. El Gamal, “The relay-eavesdropper channel: Cooperation for secrecy,” IEEE Trans. Inform. Theory, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.
[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875-1888, Mar. 2010.
[13] J. Zhang and M. C. Gursoy, “Collaborative relay beamforming for secrecy,” Proc. IEEE ICC’2010, Cape Town, May 2010.
[14] J. Li, A. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security,” IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4985-4997, Oct. 2011.
[15] S. Vishwakarma and A. Chockalingham, “Decode-and-forward relay beamforming for secrecy with finite-alphabet input,” IEEE Commun. Letters, vol. 17, no. 5, pp. 912-915, May 2013.
[16] S. Boyd and L. Vandenberghe, Convex optimization, Cambridge Univ. Press, 2004.