MIMO DF Relay Beamforming for Secrecy with Artificial Noise, Imperfect CSI, and Finite-Alphabet Input

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

Abstract—in this paper, we consider decode-and-forward (DF) relay beamforming with imperfect channel state information (CSI), cooperative artificial noise (AN) injection, and finite-alphabet input in the presence of an user and J non-colluding eavesdroppers. The communication between the source and the user is aided by a multiple-input-multiple-output (MIMO) DF relay. We use the fact that a wiretap code consists of two parts: i) common message (non-secret), and ii) secret message. The source transmits two independent messages: i) common message (non-secret), and ii) secret message. The common message is transmitted at a fixed rate $R_0$, and it is intended for the user. The secret message is also intended for the user but it should be kept secret from the $J$ eavesdroppers. The source and the MIMO DF relay operate under individual power constraints. In order to improve the secrecy rate, the MIMO relay also injects artificial noise. The CSI on all the links are assumed to be imperfect and CSI errors are assumed to be norm bounded. In order to maximize the worst case secrecy rate, we maximize the worst case link information rate to the user subject to: i) the individual power constraints on the source and the MIMO relay, and ii) the best case link information rates to $J$ eavesdroppers be less than or equal to $R_0$ in order to support a fixed common message rate $R_0$. Numerical results showing the effect of perfect/imperfect CSI, presence/absence of AN with finite-alphabet input on the secrecy rate are presented.

Keywords: MIMO relay beamforming, physical layer security, multiple eavesdroppers, artificial noise, imperfect CSI, finite-alphabet input, semi-definite programming.

I. Introduction

The physically degraded discrete memoryless wiretap channel model considered by Wyner in [1] opened the path for reliable and secure information transmission using physical layer techniques. Subsequent extension to discrete memoryless broadcast channel and Gaussian channel was done in [2] and [3], respectively. A wireless network can be easily eavesdropped due to the broadcast nature of wireless transmission. However, using physical layer techniques (e.g., wiretap codes, beamforming using multiple antennas, artificial noise injection etc.), a wireless network can be secured from getting eavesdropped. Achievable secrecy rate and capacity in single and multiple antenna wiretap channels have been reported by many authors, e.g., [4]–[9].

A relay, operating in decode-and-forward (DF) or amplify-and-forward (AF) mode, can act as an intermediate node and help improving the secrecy rate [10]. DF and AF relay beamforming techniques for secrecy under perfect/imperfect channel state information (CSI) have been well studied in the literature, e.g., [11]–[19]. In these works, the transmit codeword symbols belong to an infinite constellation (Gaussian). However, in a practical communication system, the codeword symbols will belong to a finite alphabet set, e.g., $M$-ary alphabets. The effect of finite constellation on secrecy rate has been reported in [17]–[23]. In [22], DF relay beamforming for secrecy with finite alphabet has been considered. There it was shown that when the source power and relay beamforming vector obtained for Gaussian alphabet, when used with finite alphabet, could lead to zero secrecy rate. A power control algorithm was suggested to alleviate the loss in secrecy rate. Motivated by the above works, in this paper, we consider secrecy rate in DF relay beamforming with finite-alphabet input using a MIMO relay. The considered system consists of a source node, a destination node, and multiple non-colluding eavesdroppers. A DF MIMO relay aids the communication between the source and destination. It is known that secrecy rate can be improved through the use of artificial noise (AN) injection [3], [11], [24], [25], [26]. In this work, we allow the MIMO relay to inject AN in addition to relaying the information symbol from the source. Consequently, we solve for both the optimum source power, signal beamforming weights as well as the AN covariance matrix at the MIMO relay. Since the CSI will not be perfect in practice, we consider a norm-bounded CSI error model and investigate the effect of imperfect CSI on the secrecy rate. We use the fact that a wiretap code consists of two parts: i) common message (non-secret), and ii) secret message. The source transmits two independent messages: i) common message (non-secret), and ii) secret message. The common message is transmitted at a fixed rate $R_0$, and its intended for the destination node. The secret message is also intended for the destination node but it should be kept secret from $J$ eavesdroppers. The source and the MIMO DF relay operate under individual power constraints. In order to maximize the worst case secrecy rate, we maximize the worst case link information rate to the user subject to: i) the individual power constraints on the source and the MIMO DF relay, and ii) the best case link information rates to $J$ eavesdroppers be less than or equal to $R_0$ in order to support a fixed common message rate $R_0$. Numerical results showing the effect of perfect/imperfect CSI, presence/absence of AN with finite-alphabet input on the secrecy rate are presented.

Notations: $A \in \mathbb{C}^{N_1 \times N_2}$ implies that $A$ is a complex matrix of dimension $N_1 \times N_2$. $A \succeq 0$ and $A \succ 0$ imply that $A$ is a positive semidefinite matrix and positive definite matrix, respectively. Identity matrix is denoted by $I$. Transpose
and complex conjugate transpose operations are denoted by $[.]^T$ and $[.]^*$, respectively. $E[.]$ denotes expectation operator. $\|\cdot\|$ denotes 2-norm operator. Trace of matrix $A \in \mathbb{C}^{N \times N}$ is denoted by $\text{Tr}(A)$. $\psi \in \mathbb{C}^{N \times 1} \sim \mathcal{CN}(0, \Psi)$ implies that $\psi$ is a circularly symmetric complex Gaussian random vector with mean vector $0$ and covariance matrix $\Psi$.

II. SYSTEM MODEL

Consider a DF cooperative relaying scheme which consists of a source node $S$ having single transmit antenna, a MIMO DF relay node $R$ having $N$ receive/transmit antennas, a destination node $D$ having single receive antenna, and $J$ non-colluding eavesdropper nodes $E_1, E_2, \ldots, E_J$ having single receive antenna each. The system model is shown in Fig. 1.

In addition to the links from relay to destination node and relay to eavesdropper nodes, we assume direct links from source to destination node and source to eavesdropper nodes.

The complex channel gain vector between the source and the relay is denoted by $g = [g_1, g_2, \cdots, g_N]^T \in \mathbb{C}^{N \times 1}$. Likewise, the channel gain vector between the relay and the destination node $D$ is denoted by $h = [h_1, h_2, \cdots, h_N] \in \mathbb{C}^{1 \times N}$, and the channel gain vector between the relay and the $j$th eavesdropper node $E_j$, $1 \leq j \leq J$, is denoted by $z_j = [z_{1j}, z_{2j}, \cdots, z_{Nj}] \in \mathbb{C}^{1 \times N}$. The channel gains on the direct links from the source to $D$ and the source to $E_j$ are denoted by $h_0$ and $z_{0j}$, respectively.

The MIMO relay operates in half duplex mode, and the communication happens in two hops. Each hop is divided into $n$ channel uses. We use the fact that a wire-tap code consists of two parts: $i)$ common message (non-secret), and $ii)$ secret message. 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 $\{1, 2, \cdots, 2^{2nR_c(R_0)}\}$, respectively. $W_0$ is the common message which is transmitted at a fixed rate $R_0$ and its intended for the destination $D$. $W_1$ is a secret message which is transmitted at some rate $R_s(R_0)$ and its also intended only for $D$ and it should be kept secret from all $E_j$s. For each $W_0$ and $W_1$ drawn independently and equiprobably from the sets $\{1, 2, \cdots, 2^{2nR_0}\}$ and $\{1, 2, \cdots, 2^{2nR_c(R_0)}\}$, respectively, the source $S$ maps $W_0$ and $W_1$ to a codeword $\{x_m\}_{m=1}^n$ of length $n$. Each symbol, $x_m$, in the codeword is independent and equiprobable over a complex finite-alphabet set $\mathcal{A} = \{a_1, a_2, \cdots, a_M\}$ of size $M$ with $\mathbb{E}[x_m] = 0$, and $\mathbb{E}[|x_m|^2] = 1$. The source is constrained by the available power $P_S$ and it transmits the weighted symbol which is $\sqrt{P_S}x_m$ in the $m$th channel use, where $1 \leq m \leq n$, and $0 \leq P_s \leq P_S$.

Hereafter, we will denote the symbol $x_m$ of the codeword $\{x_m\}_{m=1}^n$, by $x$, and we will consider only one channel use.

Let $y_{R}, y_{D_1}$, and $y_{E_{1j}}$ denote the received signals at the MIMO relay $R$, destination $D$, and $j$th eavesdropper $E_j$, respectively, in the first hop. We have

\[
y_{R} = \sqrt{P_S}g^tx + \eta_{R},
\]
\[
y_{D_1} = \sqrt{P_S}h_0^tx + \eta_{D_1},
\]
\[
y_{E_{1j}} = \sqrt{P_S}z_{0j}^tx + \eta_{E_{1j}},
\]

where $\eta_{R} \sim \mathcal{CN}(0, \Psi)$, $\eta_{D_1} \sim \mathcal{CN}(0, \Psi)$, and $\eta_{E_{1j}} \sim \mathcal{CN}(0, \Psi)$ are receiver noise components and are assumed to be independent.

In the second hop of transmission, MIMO relay applies the complex weight $\phi = [\phi_1, \phi_2, \cdots, \phi_N]^T \in \mathbb{C}^{N \times 1}$ on the successfully decoded symbol $x$ and retransmits it. In order to improve the secrecy rate, MIMO relay also injects the artificial noise $\psi \in \mathbb{C}^{N \times 1} \sim \mathcal{CN}(0, \Psi)$. The symbol transmitted by the MIMO relay on the $ith$ hop, $1 \leq i \leq N$, antenna is $\phi_i x + \psi_i$. Let $y_{D_2}$, and $y_{E_{2j}}$, denote the received signals at the destination $D$, and $j$th eavesdropper $E_j$, respectively, in the second hop. We have

\[
y_{D_2} = h_\phi x + h_\psi + \eta_{D_2},
\]
\[
y_{E_{2j}} = z_j^T x + z_j^T \psi + \eta_{E_{2j}},
\]

where $\eta_{D_2} \sim \mathcal{CN}(0, \Psi)$, and $\eta_{E_{2j}} \sim \mathcal{CN}(0, \Psi)$ are receiver noise components and are assumed to be independent.

Using (2), (4), and (3), (5), we rewrite the received signals at $D$ and $E_j$ in the following vector forms, respectively:

\[
y_{D} = [y_{D_1}, y_{D_2}]^T
\]
\[
= [\sqrt{P_S}h_0^tx + \eta_{D_1}, h_\phi^tx + \eta_{D_2}]^T,
\]
\[
y_{E_j} = [y_{E_{1j}}, y_{E_{2j}}]^T
\]
\[
= [\sqrt{P_S}z_{0j}^tx + \eta_{E_{1j}}, z_j^T x + z_j^T \psi + \eta_{E_{2j}}]^T.
\]

We assume that the MIMO relay’s transmit power, denoted by $P_r$, is constrained by the available power $P_R$. This implies that

\[
P_r = \mathbb{E}[\|\phi x + \psi\|^2] = \|\phi\|^2 + \text{Tr}(\Psi) \leq P_R.
\]

We also assume that the channel remains static over the entire codeword transmit duration. Further, denoting the secret message decoded at the MIMO relay $R$ and destination $D$ by $\hat{W}_1^R$ and $\hat{W}_1^D$, respectively, the reliability constraints at $R$ and $D$ and the perfect secrecy constraints at $E_j$s are as follows:

\[
\text{Pr}(\hat{W}_1^R \neq W_1) \leq \epsilon_n, \quad \text{Pr}(\hat{W}_1^D \neq W_1) \leq \epsilon_n, \quad \frac{1}{2n} I(W_1; y_{E_j}^{2n}) \leq \epsilon_n, \quad \forall j = 1, 2, \cdots, J.
\]
where \( \mathbf{y}_{E_j}^{(2)} \) is the received signal vector at \( E_j \) in 2n channel uses, and \( \epsilon_n \to 0 \) as \( n \to \infty \). We also note that the reliability constraints at the MIMO relay \( R \) and destination \( D \) for the secret message also ensure the reliability of the common message.

III. DF RELAY BEAMFORMING - PERFECT CSI

In this section, we assume that the CSI on all the links are known perfectly. Using (1), (6), and (7), we get the \( S-R, S-D, \) and \( S-E_j \) link information rates, respectively, as follows:

\[
\frac{1}{2} I(x; y_R) = \frac{1}{2} \left( \frac{P_s \| \mathbf{g} \|^2}{N_0} \right),
\]

\[
\frac{1}{2} I(x; y_D) = \frac{1}{2} \left( \frac{P_s | h_0 |^2}{N_0} + \frac{h \phi \Phi^* h^*}{N_0 + h \Psi h^*} \right),
\]

\[
\frac{1}{2} I(x; y_{E_j}) = \frac{1}{2} \left( \frac{P_s | z_{0j} |^2}{N_0} + \frac{z_j \phi \phi^* z_j^*}{N_0 + z_j \Psi z_j^*} \right),
\]

where

\[
I(x; y_R) = \frac{1}{M} \sum_{i=1}^{M} p_n(y - \sqrt{\rho a_i})
\]

\[
\frac{\log_2}{\frac{1}{M} \sum_{m=1}^{M} p_n(y - \sqrt{\rho a_m})} dy,
\]

and \( p_n(\theta) = \frac{1}{2} e^{-|\theta|^2} \). The factor \( 1/2 \) in (9), (10), and (11) is due to two hops. Further, the MIMO relay \( R \) will be able to decode the symbol \( x \) if the following condition holds true:

\[
\frac{1}{2} I(x; y_R) \geq \frac{1}{2} I(x; y_D).
\]

In order to find the maximum achievable secrecy rate \( R_s(R_0) \) which also supports the fixed common message rate \( R_0 \), we minimize the \( S-D \) link information rate subject to i) \( S-E_j \), 1 \( \leq j \leq J \), link information rates be less than or equal to \( R_0 \), ii) the information rate constraint in (13), and iii) the power constraints. The optimization problem is as follows:

\[
R_D(R_0) = \max_{P_s, \phi, \Psi} \frac{1}{2} I(x; y_D)
\]

s.t. \( \frac{1}{2} I(x; y_{E_j}) \leq R_0, \forall j = 1, 2, \ldots, J, \)

\[
0 \leq P_s \leq P_S, \quad \Psi \geq 0, \quad \| \phi \|^2 + \text{Tr}(\Psi) \leq P_R.
\]

Having obtained \( R_D(R_0) \) from (14), the maximum achievable secrecy rate \( R_s(R_0) \) for a given common message rate \( R_0 \) is

\[
R_s(R_0) = \{ R_D(R_0) - R_0 \}^+, \quad \text{(18)}
\]

For the values of \( R_0 \) over the interval \([0, R_D]\), the maximum achievable secrecy rate, denoted by \( R_s \), is obtained as follows:

\[
R_s = \max_{0 \leq R_0 \leq R_D} \{ R_D(R_0) - R_0 \}^+ \quad \text{(19)}
\]

\[
= \max_{0 \leq l \leq L} \{ R_D(\Delta_1) - l \Delta_1 \}^+, \quad \text{(20)}
\]

where \( L \) is a large positive integer, \( \Delta_1 = R_D/L, l \) is an integer, and \( R_0 = l \Delta_1 \).

We solve the optimization problem (14) for a fixed \( P_s = k \Delta_2 \), where \( \Delta_2 = P_S/K, K \) is a large positive integer, and \( 1 \leq k \leq K \). Hereafter, we will assume that \( P_s \) is known. Further, it is shown in [27,28] that for various \( M \)-ary alphabets, mutual information expression in (12) is a strictly increasing concave function in SNR. With this fact, we rewrite the optimization problem (14) into the following equivalent form:

\[
\max_{\Phi, \Psi} \left( a + \frac{h \Phi h^*}{N_0 + h \Psi h^*} \right)
\]

\[
\text{s.t.} \quad (19)
\]

\[
\text{(20)}
\]

\[
\text{(21)}
\]

\[
\text{(22)}
\]

\[
\text{(23)}
\]

\[
\text{(24)}
\]

\[
\text{(25)}
\]

\[
\Phi \succeq 0, \quad \text{rank}(\Phi) = 1, \quad \Psi \succeq 0, \quad \text{Tr}(\Phi + \Psi) \leq P_R.
\]

The above problem can be easily solved using bisection method [29]. The initial search interval in the bisection method can be taken as \([0, c]\). In the appendix, we show that the solution \( \Phi \) of the above problem has rank 1. Further, denoting the maximum value of \( t \) by \( t_{max} \), the secrecy rate is obtained as follows:

\[
R_s(R_0) = \left\{ \frac{1}{2} I(t_{max} - R_0) \right\}^+.
\]

IV. DF RELAY BEAMFORMING - IMPERFECT CSI

In this section, we assume that each receiver has perfect knowledge of its CSI. We also assume that the control unit which computes the source power, signal beamforming vector and AN covariance matrix has imperfect CSI on all links. The imperfection in CSI is modeled as follows [15,22,23,26]:

\[
g = \hat{g} + e_g, \quad h_0 = \hat{h}_0 + e_{h_0}, \quad h = \hat{h} + e_h,
\]

\[
\forall j = 1, 2, \ldots, J, \quad z_{0j} = \bar{z}_{0j} + e_{z_{0j}}, \quad z_j = \bar{z}_j + e_{z_j},
\]

\[
(\text{31})
\]
where \( \hat{g}, \hat{h}_0, \hat{h}, \bar{z}_j, \bar{z}_j \) are the available CSI estimates, and \( e_g, e_{h_0}, e_h, e_{z_0}, e_z \) are the corresponding CSI errors. We assume that the CSI errors are bounded, i.e.,

\[
\begin{align*}
\|e_g\| &\leq e_g, \quad |e_{h_0}| \leq e_{h_0}, \quad \|e_h\| \leq e_h, \\
\forall j = 1, 2, \cdots, J, \quad |e_{z_0}| &\leq e_{z_0}, \quad \|e_z\| \leq e_z.
\end{align*}
\]

(32)

With the above CSI error model, we write the rank relaxed the information rate constraint in (23), i.e., the worst case the objective function in (33) and the constraint in (36). (33) and the constraints in (35), (36), we get the following

\[
\begin{align*}
\max_{\Phi, \Psi} \min_{e_h} \left( \frac{aN_0 + (\hat{h} + e_h)(a \Psi + \Phi)(\hat{h} + e_h)^*}{N_0 + (\hat{h} + e_h)\Psi(\hat{h} + e_h)^*} \right)
\end{align*}
\]

(33)

s.t. \( \|e_h\|^2 \leq e_h^2, \) \( \forall j = 1, 2, \cdots, J, \) \( \|e_z\|^2 \leq e_z^2, \)

(34)

\[
\begin{align*}
\max \left\{ \begin{array}{l}
b_jN_0 + (\bar{z}_j + e_z)(b_j \Psi + \Phi)(\bar{z}_j + e_z)^* \\
N_0 + (\bar{z}_j + e_z)\Psi(\bar{z}_j + e_z)^*
\end{array} \right. \\
\leq I^{-1}(2R_0),
\end{align*}
\]

(35)

s.t. \( \|e_z\|^2 \leq e_z^2, \)

(36)

\[
\begin{align*}
c \geq \max_{e_h} \left( \frac{a_{\text{max}} + (\hat{h} + e_h)\Psi(\hat{h} + e_h)^*}{N_0 + (\hat{h} + e_h)\Psi(\hat{h} + e_h)^*} \right)
\end{align*}
\]

(37)

where

\[
a = \left( \frac{P_s |\hat{h}_0| - e_{h_0}}{N_0} \right)^2 \quad \text{if} \quad (|\hat{h}_0| > e_{h_0}), \quad 0, \text{ else},
\]

(38)

\[
b_j = \left( \frac{P_s |\bar{z}_0| + e_{z_0}}{N_0} \right)^2,
\]

(39)

\[
c = \left( \frac{P_s |\hat{g}| - e_g}{N_0} \right)^2 \quad \text{if} \quad (|\hat{g}| > e_g), \quad 0, \text{ else},
\]

(40)

\[
a_{\text{max}} = \left( \frac{P_s |\hat{h}_0| + e_{h_0}}{N_0} \right)^2.
\]

(41)

The objective function in (33) corresponds to the worst case \( S - D \) link information rate over the region of CSI error uncertainty. The constraint in (35) corresponds to the best case \( S - E_j \) link information rate over the region of CSI error uncertainty. The constraint in (36) is associated with the information rate constraint in (23), i.e., the worst case information rate to the MIMO relay \( R \) over the region of CSI error uncertainty should be greater than or equal to the best case information rate to destination \( D \).

Solving the optimization problem (33) is hard due to the presence of \( e_h \) in both the numerator and denominator of the objective function in (33) and the constraint in (36). Similarly, \( e_z \) appears in both the numerator and denominator of the constraint in (35). So, by independently constraining the various quadratic terms appearing in the objective function in (33) and the constraints in (35), (36), we get the following lower bound for the above optimization problem:

\[
\begin{align*}
\max_{\Phi, \Psi, e_z} \min_{e_h} \left( \frac{r_1}{r_2} \right) \\
\end{align*}
\]

(42)

s.t. \( \Phi \geq 0, \quad \Psi \geq 0, \quad \text{Tr}(\Phi + \Psi) \leq P_R, \) \( \forall e_h \) s.t. \( \|e_h\|^2 \leq e_h^2 \) \( 0 \leq r_1 \leq aN_0 + (\hat{h} + e_h)(a \Psi + \Phi)(\hat{h} + e_h)^*, \)

(44)

\[
\begin{align*}
\forall e_h \text{ s.t. } \|e_h\|^2 \leq e_h^2 \quad \Rightarrow \quad N_0 + (\hat{h} + e_h)\Psi(\hat{h} + e_h)^* \leq r_2,
\end{align*}
\]

(45)

\[
\begin{align*}
s_{\bar{z}_j} \leq I^{-1}(2R_0), \quad \forall j = 1, 2, \cdots, J,
\end{align*}
\]

(46)

\[
\begin{align*}
\forall e_z \text{ s.t. } \|e_z\|^2 \leq e_z^2 \Rightarrow \quad b_jN_0 + (\bar{z}_j + e_z)(b_j \Psi + \Phi)(\bar{z}_j + e_z)^* \leq s_{\bar{z}_j},
\end{align*}
\]

(47)

\[
\begin{align*}
\forall e_z \text{ s.t. } \|e_z\|^2 \leq e_z^2 \Rightarrow \quad 0 \leq s_{\bar{z}_j} \leq N_0 + (\bar{z}_j + e_z)\Psi(\bar{z}_j + e_z)^*.
\end{align*}
\]

(48)

The quadratic inequality constraints in (44) and (45) are associated with the objective function in (33). The constraint in (46), and the quadratic inequality constraints in (47) and (48) are associated with the constraint in (35). Similarly, the constraint in (49), and the quadratic inequality constraints in (50) and (51) are associated with the constraint in (36).

Further, using S-procedure [29], we transform the quadratic inequality constraints in (44), (45), (47), (48), (50), and (51), into the following linear matrix inequality (LMI) forms, respectively:

\[
\begin{align*}
\begin{cases}
 r_1 \geq 0, & \lambda_1 \geq 0, \quad A_1 \triangleq \\
 (a \Psi + \Phi) + \lambda_1 I & (a \Psi + \Phi)^* \\
\hat{h}(a \Psi + \Phi)^* & aN_0 + \hat{h}(a \Psi + \Phi)^* - r_1 - \lambda_1 \hat{h}^2
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
 \lambda_2 \geq 0, \quad A_2 \triangleq \\
 -\Psi - \lambda_2 I & -\Psi^* \\
 \hat{h} - \Psi & -N_0 - \hat{h}\Psi - r_2 - \lambda_2 \hat{h}^2
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
 \mu_{\bar{z}_j} \geq 0, \quad B_{\bar{z}_j} \triangleq \\
 - (b_j \Psi + \Phi) + \mu_{\bar{z}_j} I & - (b_j \Psi + \Phi)^* \\
 - \bar{z}_j (b_j \Psi + \Phi)^* & -b_jN_0 - \bar{z}_j (b_j \Psi + \Phi)^* + s_{\bar{z}_j} - \mu_{\bar{z}_j} \bar{z}_j^2
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
 \lambda_3 \geq 0, \quad A_3 \triangleq \\
 \Psi + \lambda_3 I & \Psi^* \\
 \hat{z}_j \Psi & N_0 + \hat{z}_j \Psi - s_{\bar{z}_j} - \mu_{\bar{z}_j} \bar{z}_j^2
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
 r_4 \geq 0, \quad \lambda_4 \geq 0, \quad A_4 \triangleq \\
 -\Phi - \lambda_4 I & -\Phi^* \\
 -\hat{h}\Phi & -N_0 - \hat{h}\Phi - r_3 - \lambda_4 \hat{h}^2
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
 \lambda_5 \geq 0, \quad A_5 \triangleq \\
 \Psi + \lambda_5 I & \Psi^* \\
 \hat{h}\Phi & N_0 + \hat{h}\Phi - r_4 - \lambda_5 \hat{h}^2
\end{cases}
\end{align*}
\]

where \( A_1 \geq 0, \quad A_2 \geq 0, \quad A_3 \geq 0, \quad A_4 \geq 0, \quad B_{\bar{z}_j} \geq 0, \quad B_{\bar{z}_j} \geq 0. \) We substitute the above LMI constraints in the optimization problem (42). We get the following equivalent form for the optimization problem (42):

\[
\begin{align*}
\max_{\Phi, \Psi, e_z} \min_{e_h} \left( \frac{r_1}{r_2} \right) \\
\end{align*}
\]

(42)
as discussed in Section III. The initial search interval in the rate for BPSK alphabet (i.e., perfect/imperfect CSI conditions. We assume that $J$ is seen that the secrecy rate falls approximately linearly for the MIMO relay which happens to be true for this case. The above problem can be solved using the bisection method as discussed in Section III. The initial search interval in the bisection method can be taken as $[0, c]$, where $c$ is as defined in (40). Further, denoting the maximum value of $r$ by $r_{max}$, the lower bound on the secrecy rate is obtained as follows:

$$R_s(R_0) \geq \frac{1}{2}(r_{max} - R_0)^+.$$  

(54)

V. RESULTS AND DISCUSSIONS

In this section, we present numerical results on the secrecy rate for BPSK alphabet (i.e., $M = 2$), with/without AN, perfect/imperfect CSI conditions. We assume that $N = 2$, $J = 1, 2, 3$, $N_0 = 1$, $P_s = 0$ dB, and $P_R = 9$ dB.

Perfect CSI case of Section [77]: We have used the following channel gains in the simulations:

$$g = [-0.5839 + 2.2907i, -0.7158 + 0.1144i]^T,$$

(55)

$$h_0 = -0.3822 - 0.3976i,$$

(56)

$$z_{01} = 0.0123 + 0.0137i,$$

(57)

$$z_{02} = 0.0231 - 0.0178i,$$

(58)

$$z_{03} = -0.0045 - 0.0042i,$$

(59)

$$h = [0.2174 - 0.6913i, -0.4047 - 0.3159i],$$

(60)

$$z_1 = [0.3826 + 0.0811i, 0.8389 - 0.0943i],$$

(61)

$$z_2 = [0.2977 + 0.7902i, -0.2069 + 0.4696i],$$

(62)

$$z_3 = [-0.6076 + 0.6637i, -0.3316 + 0.1921i].$$

(63)

In Fig. 2 we plot the secrecy rate versus $R_0$ for BPSK alphabet (i.e., $M = 2$), with/without AN, $J = 1, 2, 3$ eavesdroppers, $P_s = 0$ dB, and $P_R = 9$ dB. We observe that the secrecy rate initially increases with increase in $R_0$ and then drops to zero for large values of $R_0$. We also observe that the injection of AN improves the secrecy rate when $J = 2, 3$ eavesdroppers are present. However, when only one eavesdropper is present, the secrecy rate plots with/without AN overlap. This is due to the null signal beamforming by the MIMO relay at the eavesdropper. This is possible only when the number of eavesdroppers is strictly less than the number of antennas in the MIMO relay which happens to be true for this case with $N = 2$ and $J = 1$. For the case when $J = 1$, the secrecy rate maximum happens at $R_0 = 0.001445$. Further, for the case when $J = 2, 3$ and without AN, the secrecy rate maximum happens at $R_0 = 0.145797$, and with AN it happens at $R_0 = 0.080959$ and $R_0 = 0.099059$, respectively. It is seen that the secrecy rate falls approximately linearly for large $R_0$. The near-linear fall in secrecy rate for large values of $R_0$ is due to the saturation of $S-D$ link information rate to $\frac{1}{2} \log_2 2 = 0.5$ for $M = 2$. We have also numerically observed that the rank of $\Phi$ is 1.

Imperfect CSI case of Section [77]: Here, we assume that the channel gains in (55)-(63) are the available CSI estimates. We also assume that the magnitudes of the CSI errors in all the links are equal, i.e., $\epsilon_g = \epsilon_{h_0} = \epsilon_{z_{0j}} = \epsilon_h = \epsilon_{z_j} = \epsilon$. We solve the optimization problem (52) for BPSK alphabet (i.e., $M = 2$), with AN, fixed $P_s = 0.0810$, $P_s = 0$ dB, and $P_R = 9$ dB. In Fig. 3 we plot $R_s$ vs $c$ with AN for $J = 1, 2, 3$. We observe that the secrecy rate decreases with increase in CSI error and with increase in number of eavesdroppers. We have also numerically observed that the rank of $\Phi$ is 1.

VI. CONCLUSIONS

We considered MIMO DF relay beamforming with imperfect CSI, cooperative artificial noise injection, and finite-alphabet input in the presence of an user and multiple non-colluding eavesdroppers. The source transmits common and secret messages which are intended for the user. The common message is transmitted at a fixed rate $R_0$. In order to maximize the worst case secrecy rate, we maximized the worst case link information rate to the user subject to: i) the individual power constraints on the source and the MIMO DF relay, and ii) the best case link information rates to $J$ eavesdroppers be less than or equal to $R_0$ in order to support a fixed common message rate $R_{0o}$. Numerical results showing the effect of perfect/imperfect CSI, presence/absence of AN with finite-alphabet input on the secrecy rate were presented. We would like to remark that the work presented in this paper can be extended to amplify-and-forward relay channel.
Appendix

In this appendix, we analyze the rank of the optimal solution \( \Phi \) obtained from the optimization problem (25). We take the Lagrangian of the objective function \( -t \) with constraints in (26)-(29) as follows [29]:

\[
\ell(t, \Phi, \Psi, \lambda, A_1, A_2, \mu, \nu_j, \xi) = -t - \text{Tr}(A_1 \Phi) - \text{Tr}(A_2 \Psi) + \lambda \left( \text{Tr}(\Phi) + \text{Tr}(\Psi) - P_R \right) \\
+ \mu \left( (t - a) (N_0 + h \Psi h^*) - (h \Phi h^*) \right) \\
+ \sum_{j=1}^{J} \nu_j \left( (z_j \Phi z_j^*) - \left( I^{-1}(2R_0) - b_j \right) (N_0 + z_j \Psi z_j^*) \right) \\
+ \xi \left( (h \Phi h^*) - (c - a) (N_0 + h \Psi h^*) \right)
\]  

(64)

where \( \lambda \geq 0, A_1 \geq 0, A_2 \geq 0, \mu \geq 0, \nu_j \geq 0, \xi \geq 0 \) are Lagrangian multipliers. The KKT conditions for (64) are as follows:

(a1) all constraints in (26)-(29),

(a2) \( \text{Tr}(A_1 \Phi) = 0 \). Since \( A_1 \geq 0 \) and \( \Phi \geq 0 \) \( \implies \ A_1 \Phi = 0 \),

(a3) \( \text{Tr}(A_2 \Psi) = 0 \). Since \( A_2 \geq 0 \) and \( \Psi \geq 0 \) \( \implies \ A_2 \Psi = 0 \),

(a4) \( \lambda \left( \text{Tr}(\Phi) + \text{Tr}(\Psi) - P_R \right) = 0 \),

(a5) \( \mu \left( (t - a) (N_0 + h \Psi h^*) - (h \Phi h^*) \right) = 0 \),

(a6) \( \forall j = 1, 2, \ldots, J, \nu_j \left( (z_j \Phi z_j^*) - \left( I^{-1}(2R_0) - b_j \right) (N_0 + z_j \Psi z_j^*) \right) = 0 \).

(a7) \( \xi \left( (h \Phi h^*) - (c - a) (N_0 + h \Psi h^*) \right) = 0 \),

(a8) \( \frac{\partial \ell}{\partial \Psi} = 0 \implies \mu (N_0 + h \Psi h^*) = 1 \). This further implies that \( \mu > 0 \),

(a9) \( \frac{\partial \ell}{\partial \Phi} = 0 \implies A_1 = \lambda I - \mu (h^* h) + \sum_{j=1}^{J} \nu_j (z_j^* z_j) + \xi (h^* h) \),

(a10) \( \frac{\partial \ell}{\partial h} = 0 \implies \Lambda_2 = \lambda I + \mu (t - a) (h^* h) - \sum_{j=1}^{J} \nu_j \left( I^{-1}(2R_0) - b_j \right) (z_j^* z_j) - \xi (c - a) (h^* h) \).

The KKT conditions (a8) and (a5) imply that the constraint (26) will be satisfied with equality. Assuming \( \Phi \neq 0 \), this further implies that \( t > a \). The constraints (27) and (28) imply that \( I^{-1}(2R_0) \geq b_j \) and \( c > a \). The KKT conditions (a9), (a10), (a2), (a3), (a4), (a5), and (a7) imply that

\[
\lambda P_R - \mu (t - a) N_0 + \sum_{j=1}^{J} \nu_j \left( I^{-1}(2R_0) - b_j \right) N_0 \\
+ \xi (c - a) N_0 = 0.
\]  

(65)

Let \( P_R \) be small enough such that the constraint in (28) is satisfied with strict inequality. This implies that the KKT condition (a7) will be satisfied only when \( \xi = 0 \). With \( \xi = 0 \), we consider the scenario when the expression (65) is satisfied for \( \lambda > 0 \). With \( \lambda > 0 \), the KKT condition (a4) implies that \( \text{Tr}(\Phi) + \text{Tr}(\Psi) = P_R \), i.e., the entire relay power, \( P_R \), will be used for transmission. Further, we rewrite the KKT condition (a9) as follows:

\[
\Lambda_1 + \mu (h^* h) = \lambda I + \sum_{j=1}^{J} \nu_j (z_j^* z_j) > 0.
\]  

(66)

The above expression implies that \( \text{rank}(\Lambda_1) \geq N - \text{rank}(\mu (h^* h)) = N - 1 \). The KKT condition (a2) further implies that \( \text{rank}(\Phi) = N - 1 \) and \( \text{rank}(\Psi) = 1 \).

We now show that the solution \( \Phi \) of the optimization problem (25) has rank-1 even for large values of \( P_R \). Let \( \Phi \neq 0 \) (\( \geq 0 \)) and \( \Psi \neq 0 \) (\( \geq 0 \)) be the optimal solutions of (25) with \( \text{Tr}(\Phi) + \text{Tr}(\Psi) = P \leq P_R \), and the objective function value \( t > 0 \). Define

\[
\Phi_0 = \frac{\Phi}{\text{Tr}(\Phi) + \text{Tr}(\Psi)} \quad \text{and} \quad \Psi_0 = \frac{\Psi}{\text{Tr}(\Phi) + \text{Tr}(\Psi)}.
\]

It is obvious that the objective function value, \( t \), in the optimization problem (25) is a non-decreasing function in \( P_R \). As discussed previously for small values of \( P_R \), the optimization problem (25) attains its maximum value when entire power is used, i.e., \( \Phi_0, \Psi_0 = (P_R \Phi_0, P_R \Psi_0) \). This implies that the objective function value, \( t \), in (25) is a strictly increasing function in \( P_R \) for small values of \( P_R \). We now fix the directional matrices \( \Phi_0, \Psi_0 \) which are obtained for small values of \( P_R \) such that the constraint in (28) is satisfied with strict inequality. We rewrite the constraints in (27) and (28) in the following inequalities, respectively:
\[ j = 1, 2, \ldots, J, \quad I^{-1}(2R_0) \geq \left( b_j + \frac{z_j \Phi z_j^*}{N_0 + z_j \Psi z_j^*} \right). \quad (67) \]

\[ c \geq \left( a + \frac{h_j \Phi h_j^*}{N_0 + h_j \Psi h_j^*} \right). \quad (68) \]

In the above inequalities, the derivatives of the functions \( \frac{z_j \Phi z_j^*}{N_0 + z_j \Psi z_j^*} \) and \( \frac{h_j \Phi h_j^*}{N_0 + h_j \Psi h_j^*} \) w.r.t. \( P \) when evaluated at \((P \Phi_0, P \Psi_0)\) are \( \geq 0 \) and \( > 0 \), respectively. This implies that the right hand sides of the inequalities in (67) and (68) are non-decreasing and strictly increasing functions in \( P \), respectively, at \((P \Phi_0, P \Psi_0)\). This further implies that if the above inequalities are satisfied at \((P_R \Phi_0, P_R \Psi_0)\), the optimization problem \((25)\) will attain its maximum value at \((P_R \Phi_0, P_R \Psi_0)\), i.e., when the entire available relay power, \( P_R \), is used. When \( P_R \) is large such that the above inequalities fail to satisfy at \((P_R \Phi_0, P_R \Psi_0)\), the optimization problem \((25)\) will attain its maximum value at \((P \Phi_0, P \Psi_0)\), where \( P \) \((< P_R)\) is the maximum power at which the above inequalities are satisfied at \((P \Phi_0, P \Psi_0)\). The excess power \((P_R - P)\) will remain unused. This implies that the ranks of \( \Phi \) and \( \Psi \) remain constant for large values of \( P_R \).

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. Körner, “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 channel,”IEEE Trans. Inform. Theory, vol. IT-24, pp. 451-456, Jul. 1978.

[4] S. Shafigue and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraint,”Proc. IEEE ISIT’2007, Jun. 2007.

[5] A. Khisti and G. Wornell, “Secure transmission with multiple antennas-I: The MISO wiretap channel,”IEEE Trans. Inform. Theory, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[6] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,”Proc. IEEE ISIT’2008, Jul. 2008.

[7] 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.

[8] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,”IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[9] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wiretap channels,”EURASIP Journ. on Wireless Commun. and Net., volume 2009, article ID 142374, 12 pages. doi:10.1155/2009/142374.

[10] 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.

[11] 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.

[12] J. Zhang and M. C. Gursoy, “Collaborative relay beamforming for secrecy,”Proc. IEEE PIMRC’2010, Sep. 2010.

[13] J. Zhang and M. C. Gursoy, “Relay beamforming strategies for physical-layer security,”Proc. CISS’2010, Mar. 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. Chockalingam, “Decode-and-forward relay beamforming for secrecy with imperfect CSI and multiple eavesdroppers,”Proc. IEEE SPAWC’2012, Jun. 2012.

[16] S. Vishwakarma and A. Chockalingam, “MIMO decode-and-forward relay beamforming for secrecy with cooperative jamming,”Proc. National Conf. Commun. (NCC’2014), Kanpur, Feb. 2014.

[17] M. R. D. Rodrigues, A. S. Baruch, and M. Bloch, “On Gaussian wiretap channels with M-PAM inputs,”2010 European Wireless Conf., pp.774-781, Apr. 2010.