Securing Downlink Non-Orthogonal Multiple Access Systems by Trusted Relays

Ahmed Arafa[1], Wonjae Shin[2,1], Mojtaba Vaezi[3,1], and H. Vincent Poor[1]

[1]Electrical Engineering Department, Princeton University
[2]Department of Electronics Engineering, Pusan National University
[3]Electrical and Computer Engineering Department, Villanova University

Abstract—A downlink single-input single-output non-orthogonal multiple access system is considered in which a base station (BS) is communicating with two legitimate users in the presence of an external eavesdropper. A group of trusted cooperative half-duplex relay nodes, powered by the BS, is employed to assist the BS's transmission. The goal is to design relaying schemes such that the legitimate users' *secrecy rate region* is maximized subject to a total power constraint on the BS and the relays' transmissions. Three relaying schemes are investigated: *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward*. Depending on the scheme, *secure beamforming* signals are carefully designed for the relay nodes that either diminish the eavesdropper's rate without affecting that of the legitimate users, or increase the legitimate users' rates without increasing that of the eavesdropper. The results show that there is no relaying scheme that fits all conditions; the best relaying scheme depends on the system parameters, namely, the relays' and eavesdropper's distances from the BS, and the number of relays. They also show that the relatively simple cooperative jamming scheme outperforms other schemes when the relays are far from the BS and/or close to the eavesdropper.

I. INTRODUCTION

Non-orthogonal multiple access (NOMA) systems are leading candidates for future mobile communications, as they provide an efficient means of utilizing resources serving multiple users simultaneously compared to orthogonal multiple access schemes [1]. With the inherent broadcast nature of wireless communications, securing transmitted data is critical in the presence of potential eavesdroppers in the medium. Physical layer security is a powerful, and provably unbreakable, technique to deliver secure data as opposed to conventional security techniques implemented in higher layers of the communication protocol stack; see, e.g., [2] and the references therein. In this work, we focus on enhancing physical layer security of single-input single-output (SISO) NOMA systems by using cooperative relays.

There have been a number of recent works that study physical layer security for NOMA systems [3]–[11]. Secrecy sum rate maximization of SISO NOMA systems is studied in [3]. Using tools from stochastic geometry, references [4] and [5] study security measures for large scale NOMA systems in the downlink and uplink, respectively. NOMA assisted multicast-unicast streaming is studied in [6], where secure
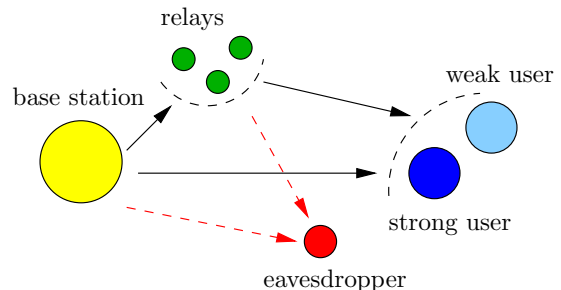
Fig. 1. Downlink NOMA system model, with cooperative relays, and an external eavesdropper.

rates for unicast transmission using NOMA is shown to outperform conventional orthogonal schemes. Reference [7] considers a multiple-input multiple-output (MIMO) two-user NOMA setting with an external eavesdropper and designs beamforming signals that maximize the secrecy sum rate. This approach is also considered in [8] and [9] for multiple-input single output and MIMO scenarios, respectively, with the assumption that one user is entrusted and the other is the potential eavesdropper. The impact of transmit antenna selection strategies on the secrecy outage probability is investigated in [10]. Transmit power minimization and minimum secrecy rate maximization subject to a secrecy outage constraint is considered in [11].

Our work is most closely related to [12], where relays are used to enhance the secrecy rate of a single-receiver wiretap channel. In this paper, we extend the ideas in [12] to work in the context of a two-user downlink SISO NOMA system with an external eavesdropper. We employ multiple *trusted cooperative* half-duplex relays to enhance the achievable secrecy rate region through various relaying schemes: *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward*. For each scheme, we design *secure beamforming* signals at the relays that benefit the users and/or hurt the eavesdropper. Under a total system power constraint, which is divided between the base station (BS) and the relays, an achievable secrecy rate region for each relaying scheme is derived and analyzed. In general, the results show that the best relaying scheme highly depends on the system parameters, in particular the distances between nodes, and that the relatively simple cooperative jamming scheme performs better than the other schemes when the relays are close to the eavesdropper.

II. SYSTEM MODEL

We consider a two-user downlink SISO NOMA system in which the BS uses superposition coding to send messages to the two users simultaneously. User channels are fixed during the communication session and are known at the BS. The user with a relatively worse channel condition (weak user) decodes its message by treating the other user's interfering signal as noise, while the user with a relatively better channel condition (strong user) first decodes the weak user's message, by treating its own signal as noise, and then uses successive interference cancellation to decode its own message[1].

We denote the channel between the BS and the strong user (resp. weak user) by h_1 (resp. h_2), with[2] $|h_1|^2 > |h_2|^2$. The received signals at the strong and weak users are given by

$$y_1 = h_1 x + n_1 \tag{1}$$
$$y_2 = h_2 x + n_2 \tag{2}$$

where the noise terms n_1 and n_2 are independent and identically distributed (i.i.d.) circularly-symmetric complex Gaussian random variables with zero means and unit variances, $\mathcal{CN}(0,1)$, and the transmitted signal x is given by

$$x = \sqrt{\alpha P} s_1 + \sqrt{\bar{\alpha} P} s_2 \tag{3}$$

where s_1 and s_2 are i.i.d. $\sim \mathcal{CN}(0,1)$ information carrying signals for the strong and the weak user, respectively, P is the BS's transmit power budget, $\alpha \in [0,1]$ is the fraction of power allocated to the strong user, and $\bar{\alpha} \triangleq 1 - \alpha$. Using superposition coding and successive interference cancellation decoding, one achieves the following rates of this (degraded) Gaussian broadcast channel [13]:

$$r_1 = \log\left(1 + |h_1|^2 \alpha P\right) \tag{4}$$
$$r_2 = \log\left(1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P}\right). \tag{5}$$

An external eavesdropper is monitoring the communication between the BS and the users. We denote the channel between the BS and the eavesdropper by h_e. Thus, the received signal at the eavesdropper is given by

$$y_e = h_e x + n_e \tag{6}$$

where the noise term $n_e \sim \mathcal{CN}(0,1)$. For a given $0 \leq \alpha \leq 1$, the secrecy capacities of the two users of this multi receiver wiretap channel is given by [14, Theorem 5]

$$r_{s,1} = \left[\log\left(1 + |h_1|^2 \alpha P\right) - \log\left(1 + |h_e|^2 \alpha P\right)\right]^+ \tag{7}$$
$$r_{s,2} = \left[\log\left(1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P}\right) - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P}\right)\right]^+ \tag{8}$$

where the subscript s, here and throughout the paper, is to denote secrecy rates, and $[x]^+ \triangleq \max\{x, 0\}$.

[1]The two-user setting in this work is adopted in NOMA systems in which users are divided into multiple clusters with two users each, in order to reduce error propagation in successive interference cancellation decoding [1].

[2]All channel gains in this paper are complex-valued, and are drawn independently from some continuous distribution.

It is clear from (7) and (8) that sending secure data depends on the eavesdropper's channel condition with respect to that of the legitimate users. Therefore, we propose using trusted cooperative half-duplex *relay* nodes, see Fig. 1, to assist the BS via three possible schemes: *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward*. In all of these schemes, the BS uses only a portion of its available power $\bar{P} \leq P$ for its own transmission, and shares the remaining portion $P - \bar{P}$ with the relays for their transmission. We discuss these schemes in detail in the following sections, after introducing the relays' channels notation that we use.

Let there be K relays, and denote the channel gains from the BS to the relays by the vector[3] $\boldsymbol{h}_r \triangleq [h_{r,1}, \ldots, h_{r,K}]$. Let $\boldsymbol{g}_1$, $\boldsymbol{g}_2$, and $\boldsymbol{g}_e$ denote the K-length channel gain vectors from the relays to the first user, the second user, and the eavesdropper, respectively. The channels from the relays to the users and the eavesdropper are known at the relays.

III. COOPERATIVE JAMMING

In this section, we discuss the cooperative jamming scheme. *Simultaneously* with the BS's transmission, the relays transmit a cooperative jamming signal $\boldsymbol{J}z$, where $\boldsymbol{J} \in \mathbb{C}^K$ is a beamforming vector and $z \sim \mathcal{CN}(0,1)$. The received signals at the users and the eavesdropper are in this case given by

$$y_j = h_j x + \boldsymbol{g}_j^\dagger \boldsymbol{J}z + n_j, \quad j = 1, 2, e \tag{9}$$

where the superscript $\dagger$ denotes the conjugate transpose operation. The signal power is now set to $\mathbb{E}\left[|x|^2\right] = \bar{P} \leq P$, where $\mathbb{E}[\cdot]$ denotes expectation, and the remaining portion $P - \bar{P}$ is used to power the relays, i.e., $\mathbb{E}\left[(\boldsymbol{J}z)^\dagger(\boldsymbol{J}z)\right] = \boldsymbol{J}^\dagger \boldsymbol{J} = P - \bar{P}$.

The design of the jamming signal is such that it has minimal effect on the legitimate users as follows:

$$\begin{bmatrix} \boldsymbol{g}_1 & \boldsymbol{g}_2 \end{bmatrix}^\dagger \boldsymbol{J} \triangleq \boldsymbol{G}^\dagger \boldsymbol{J} = \begin{bmatrix} 0 & 0 \end{bmatrix}. \tag{10}$$

That is, we choose $\boldsymbol{J}$ in the null space of the matrix $\boldsymbol{G}^\dagger$. If there exist $K \geq 3$ relays, then $\boldsymbol{G}^\dagger$ will always have a nonempty null space and (10) will have a nontrivial solution. We denote such a null space jamming signal by $\boldsymbol{J}_o$. Since the channel state vectors $\boldsymbol{g}_1$, $\boldsymbol{g}_2$, and $\boldsymbol{g}_e$ are drawn from a continuous distribution, they are therefore linearly independent with probability 1 (w.p. 1). Thus, we have

$$\left|\boldsymbol{g}_e^\dagger \boldsymbol{J}_o\right| > 0, \quad \text{w.p. 1}. \tag{11}$$

Therefore, the achievable secrecy rates are now given by (7) and (8) after replacing h_e with $\tilde{h}_e$ which is given by

$$\tilde{h}_e \triangleq h_e \Big/ \left(1 + \left|\boldsymbol{g}_e^\dagger \boldsymbol{J}_o\right|^2\right). \tag{12}$$

We now find the optimal $\boldsymbol{J}_o$ that maximally degrades the eavesdropper's channel subject to not affecting the legitimate users' channels. Observe that both legitimate users' rates are decreasing in $\tilde{h}_e$, i.e., increasing in $\left|\boldsymbol{g}_e^\dagger \boldsymbol{J}_o\right|^2$. Therefore, to

[3]All vectors in this paper are column vectors.

maximize their secrecy rates, we formulate the following optimization problem for a given transmit power $\bar{P}$:

$$\max_{\boldsymbol{J}_o} \quad \left| \boldsymbol{g}_e^\dagger \boldsymbol{J}_o \right|^2$$
$$\text{s.t.} \quad \boldsymbol{G}^\dagger \boldsymbol{J}_o = \begin{bmatrix} 0 & 0 \end{bmatrix}, \; \boldsymbol{J}_o^\dagger \boldsymbol{J}_o = P - \bar{P}. \quad (13)$$

The above problem has a unique solution [15] (see also [12]), which we derive next for completeness. We first rewrite the first constraint slightly differently as follows:

$$\boldsymbol{J}_o = \mathcal{P}^\perp (\boldsymbol{G}) \, \boldsymbol{u}_J \quad (14)$$

for some vector $\boldsymbol{u}_J \in \mathbb{C}^K$ to be designed, and $\mathcal{P}^\perp (\boldsymbol{G})$ is the orthogonal projection matrix onto the null space of $\boldsymbol{G}^\dagger$:

$$\mathcal{P}^\perp (\boldsymbol{G}) \triangleq \boldsymbol{I}_K - \boldsymbol{G} \left(\boldsymbol{G}^\dagger \boldsymbol{G} \right)^{-1} \boldsymbol{G}^\dagger \quad (15)$$

where $\boldsymbol{I}_K$ is the K-dimensional identity matrix. It is now direct to see that the vector $\boldsymbol{u}_J$ should be chosen along the same direction of $\mathcal{P}^\perp (\boldsymbol{G}) \, \boldsymbol{g}_e$ in order to maximize $\left| \boldsymbol{g}_e^\dagger \boldsymbol{J}_o \right|^2$. Finally, to satisfy the power constraint, the optimal beamforming vector, $\hat{\boldsymbol{J}}_o$, is given by

$$\hat{\boldsymbol{J}}_o = \frac{\mathcal{P}^\perp (\boldsymbol{G}) \, \boldsymbol{g}_e}{\left\| \mathcal{P}^\perp (\boldsymbol{G}) \, \boldsymbol{g}_e \right\|} \sqrt{P - \bar{P}} \quad (16)$$

which, upon substituting in (12), achieves the following secrecy rates for a given $\bar{P}$ and α:

$$r_{s,1}^J = \left[\log \left(1 + |h_1|^2 \alpha \bar{P} \right) \right.$$
$$\left. - \log \left(1 + \frac{|h_e|^2 \alpha \bar{P}}{1 + \boldsymbol{g}_e^\dagger \mathcal{P}^\perp (\boldsymbol{G}) \, \boldsymbol{g}_e \left(P - \bar{P} \right)} \right) \right]^+ \quad (17)$$

$$r_{s,2}^J = \left[\log \left(1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}} \right) \right.$$
$$\left. - \log \left(1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P} + \boldsymbol{g}_e^\dagger \mathcal{P}^\perp (\boldsymbol{G}) \, \boldsymbol{g}_e \left(P - \bar{P} \right)} \right) \right]^+ \quad (18)$$

with the superscript J denoting cooperative jamming.

In Section VI, we discuss the evaluation of the optimal transmit power $\bar{P}$ and the power fraction α that maximize the secrecy rate region of this cooperative jamming scheme, along with those that maximize the secrecy rate regions of the other relaying schemes that we consider in this paper.

IV. Decode-and-Forward

In this section, we discuss the decode-and-forward scheme. Different from the cooperative jamming scheme, communication takes place over two phases. In the first phase, the BS broadcasts the messages to both the relays and the legitimate users. In the second phase, the relays forward the messages that they decoded to the legitimate users. The eavesdropper overhears the communication during both phases.

The received signals during the first phase at the legitimate users and the eavesdropper are given by (1)–(2) and (6), respectively, with a total transmit power $\bar{P} \leq P$. The received signals at the relays during the first phase is given by

$$\boldsymbol{y}_r = \boldsymbol{h}_r x + \boldsymbol{n}_r \quad (19)$$

where the noise term vector $\boldsymbol{n}_r \sim \mathcal{CN}(0, \boldsymbol{I}_K)$. During the first phase, each relay decodes the users' messages by either decoding the weak user's message first by treating the strong user's signal as noise, and then decoding the strong user's message via successive interference cancellation, or it can do the whole process in the reverse order by decoding the strong user's message first followed by that of the weak user. Choosing the decoding order depends on in which part of the rate region the system is operating. For simplicity, we let all the relays choose the same decoding order, i.e., they all take one collective decision on that matter. Let the superscript (i), $i = 1, 2$, denote the ith decoding order, with $i = 1$ denoting decoding the strong user's message first followed by that of the weak user, and $i = 2$ denoting the reverse order. Thus, the achieved rate pairs at the kth relay after the first phase are either given as follows for $i = 1$:
$$\left(R_{k,1}^{(1)}, R_{k,2}^{(1)} \right) = \left(\log \left(1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}} \right), \log \left(1 + |h_{r,k}|^2 \bar{\alpha} \bar{P} \right) \right),$$
or are given as follows for $i = 2$:
$$\left(R_{k,1}^{(2)}, R_{k,2}^{(2)} \right) = \left(\log \left(1 + |h_{r,k}|^2 \alpha \bar{P} \right), \log \left(1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}} \right) \right).$$

In the second phase, the relays form the transmitted signal x_r, which is exactly as in (3) but after replacing P with $P - \bar{P}$. We assume that the relays use the same power fraction α in the second phase. While in general each relay can use a different power fraction, we use the same fraction for simplicity of presentation of the scheme hereafter. The relays use a unit-norm beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$ during the second phase, i.e., the kth relay multiplies the transmitted signal x_r by d_k and sends it through the channel, and hence the received signals at the legitimate users and the eavesdropper are given by

$$y_j^r = \boldsymbol{g}_j^\dagger \boldsymbol{d} x_r + n_j^r, \quad j = 1, 2, e \quad (20)$$

where the superscript r is to denote signals received from the relays, and the noise terms n_1^r, n_2^r, and n_e^r are i.i.d. $\sim \mathcal{CN}(0, 1)$. We let the relays use independent codewords from those used by the BS to forward their messages. The achieved rates at the legitimate users after the second phase are given by (21) and (22) at the top of the next page [16, Theorem 16.2], given that the relays follow the decoding order (i), with the superscript DF denoting decode-and-forward.

For $K \geq 2$, we design the beamforming vector $\boldsymbol{d}$ to be a unit-norm vector orthogonal to $\boldsymbol{g}_e$, and denote it by $\boldsymbol{d}_o$. This way, the eavesdropper does not gain any useful information during the second phase. Thus, we have

$$\boldsymbol{g}_e^\dagger \boldsymbol{d}_o = 0. \quad (23)$$

Further, for $K \geq 3$, we have that $\{\boldsymbol{g}_1, \boldsymbol{g}_2, \boldsymbol{g}_e\}$ are linearly independent w.p. 1, and hence

$$|\boldsymbol{g}_1^\dagger \boldsymbol{d}_o| > 0, \; |\boldsymbol{g}_2^\dagger \boldsymbol{d}_o| > 0, \quad \text{w.p. 1}. \quad (24)$$

Thus, the achievable secrecy rates in this case are given by

$$r_{s,1}^{DF} = \frac{1}{2} \left[r_1^{DF} - \log \left(1 + |h_e|^2 \alpha \bar{P} \right) \right]^+ \quad (25)$$

$$r_{s,2}^{DF} = \frac{1}{2} \left[r_2^{DF} - \log \left(1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P}} \right) \right]^+ \quad (26)$$

$$r_1^{DF} = \min\left\{\log\left(1 + |h_1|^2\alpha\bar{P}\right) + \log\left(1 + \left|g_1^\dagger d\right|^2\alpha\left(P - \bar{P}\right)\right), \min_{1\leq k\leq K} R_{k,1}^{(i)}\right\} \tag{21}$$

$$r_2^{DF} = \min\left\{\log\left(1 + \frac{|h_2|^2\bar{\alpha}\bar{P}}{1 + |h_2|^2\alpha\bar{P}}\right) + \log\left(1 + \frac{\left|g_2^\dagger d\right|^2\bar{\alpha}\left(P - \bar{P}\right)}{1 + \left|g_2^\dagger d\right|^2\alpha\left(P - \bar{P}\right)}\right), \min_{1\leq k\leq K} R_{k,2}^{(i)}\right\} \tag{22}$$

---

where the extra multiplication by $\frac{1}{2}$ is due to transmission of the same message over two phases with equal durations.

We now optimize the beamforming vector d_o. Towards that end, we rewrite the constraint in (23) slightly differently as

$$d_o = \mathcal{P}^\perp(g_e)\, u_d \tag{27}$$

where $\mathcal{P}^\perp(\cdot)$, as defined in (15), now represents a projection matrix onto the orthogonal complement of vectors in $\mathbb{C}^K$, and $u_d \in \mathbb{C}^K$ is some vector to be designed. Next, it is direct to see that r_1^{DF} is non-decreasing in $\left|g_1^\dagger d_o\right|^2$ and that r_2^{DF}, after simple first derivative analysis, is non-decreasing in $\left|g_2^\dagger d_o\right|^2$. Hence, one needs to choose d_o to maximize these terms. We propose maximizing their convex combination $\beta\left|g_1^\dagger d_o\right|^2 + (1 - \beta)\left|g_2^\dagger d_o\right|^2$, for some $0 \leq \beta \leq 1$ of choice. Using (27), and after simple manipulations, the optimal $\hat{u}_d$ is given by the solution of the following problem:

$$\max_{u_d}\quad u_d^\dagger\mathcal{P}^\perp(g_e)\left(\beta g_1 g_1^\dagger + (1 - \beta)g_2 g_2^\dagger\right)\mathcal{P}^\perp(g_e)\, u_d$$

$$\text{s.t.}\quad u_d^\dagger\mathcal{P}^\perp(g_e)\, u_d = 1 \tag{28}$$

and therefore $\hat{u}_d$ is given by the leading eigenvector of the (Hermitian) matrix:

$$\mathcal{P}^\perp(g_e)\left(\beta g_1 g_1^\dagger + (1 - \beta)g_2 g_2^\dagger\right)\mathcal{P}^\perp(g_e) \tag{29}$$

i.e., the eigenvector corresponding to its largest eigenvalue. Finally, the optimal $\hat{d}_o$ is given by

$$\hat{d}_o = \frac{\mathcal{P}^\perp(g_e)\,\hat{u}_d}{\|\mathcal{P}^\perp(g_e)\,\hat{u}_d\|}. \tag{30}$$

Substituting $\hat{d}_o$ in (25) and (26) gives the secrecy rates.

V. Amplify-and-Forward

In this section, we discuss the amplify-and-forward scheme. As in the decode-and-forward scheme, communication takes place over two phases. In the first phase, the received signals at the legitimate users, eavesdropper, and relays are given by (1)–(2), (6), and (19), respectively, with a total transmit power $\bar{P} \leq P$. In the second phase, the kth relay amplifies its received signal by multiplying it by a constant a_k and sends it through the channel. Effectively, this can be written as the multiplication $\mathtt{diag}(a)\, y_r$, where $a \in \mathbb{C}^K$ is a beamforming vector to be designed, and $\mathtt{diag}(a)$ is a diagonalization of the vector a. The received signals at the legitimate users and the eavesdropper in the second phase are given by

$$y_j^r = g_j^\dagger\mathtt{diag}(a)\, y_r + n_j^r, \quad j = 1, 2, e. \tag{31}$$

Now observe that from, e.g., the strong user's perspective, this amplify-and-forward scheme can be viewed, using (19), as the following single-input multiple-output (SIMO) system:

$$\begin{bmatrix} y_1 \\ y_1^r \end{bmatrix} = \begin{bmatrix} h_1 \\ g_1^\dagger\mathtt{diag}(a)\, h_r \end{bmatrix} x + \begin{bmatrix} n_1 \\ \tilde{n}_1^r \end{bmatrix} \tag{32}$$

where the noise term $\tilde{n}_1^r \triangleq g_1^\dagger\mathtt{diag}(a)\, n_r + n_1^r$ is complex-Gaussian with zero mean and variance $\mathbb{E}\left[|\tilde{n}_1^r|^2\right] = g_1^\dagger\mathtt{diag}(a^*)\,\mathtt{diag}(a)\, g_1 + 1$, with the superscript $*$ denoting the conjugate operation. One can write similar equations for the weak user as well. Hence, the achievable rates at the legitimate users of this SIMO system after the second phase are given by [17, Section 5.3.1]

$$r_1^{AF} = \log\left(1 + |h_1|^2\alpha\bar{P} + \frac{a^\dagger G_{1,r}a}{1 + a^\dagger G_1 a}\alpha\bar{P}\right) \tag{33}$$

$$r_2^{AF} = \log\left(1 + \frac{|h_2|^2\bar{\alpha}\bar{P}}{1 + |h_2|^2\alpha\bar{P}} + \frac{a^\dagger G_{2,r}a\bar{\alpha}\bar{P}}{1 + a^\dagger G_2 a + a^\dagger G_{2,r}a\alpha\bar{P}}\right) \tag{34}$$

with the superscript AF denoting amplify-and-forward, and

$$G_{j,r} \triangleq \mathtt{diag}(h_r^*)\, g_j g_j^\dagger\mathtt{diag}(h_r), \quad j = 1, 2 \tag{35}$$

$$G_j \triangleq \mathtt{diag}(g_j^*)\,\mathtt{diag}(g_j), \quad j = 1, 2. \tag{36}$$

As for the eavesdropper, observe that by (19) we have

$$g_e^\dagger\mathtt{diag}(a)\, y_r = g_e^\dagger\mathtt{diag}(a)\, h_r x + g_e^\dagger\mathtt{diag}(a)\, n_r. \tag{37}$$

Upon noting that $g_e^\dagger\mathtt{diag}(a)\, h_r = g_e^\dagger\mathtt{diag}(h_r)\, a$, we propose, for $K \geq 2$, designing the beamforming vector a to be orthogonal to the vector $\mathtt{diag}(h_r^*)\, g_e$ and denote it by a_o. This way, the eavesdropper does not gain any useful information during the second phase. Thus, we have

$$g_e^\dagger\mathtt{diag}(h_r)\, a_o = 0. \tag{38}$$

As in the decode-and-forward scheme, we have for $K \geq 3$ that $\{g_1, g_2, g_e\}$ are linearly independent w.p. 1. Hence

$$|g_1^\dagger\mathtt{diag}(h_r)\, a_o| > 0, \; |g_2^\dagger\mathtt{diag}(h_r)\, a_o| > 0, \; \text{w.p. 1.} \tag{39}$$

Thus, the achievable secrecy rates in this case are given by

$$r_{s,1}^{AF} = \frac{1}{2}\left[r_1^{AF} - \log\left(1 + |h_e|^2\alpha\bar{P}\right)\right]^+ \tag{40}$$

$$r_{s,2}^{AF} = \frac{1}{2}\left[r_2^{AF} - \log\left(1 + \frac{|h_e|^2(1 - \alpha)\bar{P}}{1 + |h_e|^2\alpha\bar{P}}\right)\right]^+ \tag{41}$$

where the extra multiplication by $\frac{1}{2}$ is due to transmission of the same message over two phases of equal durations.

We now focus on further optimizing the beamforming signal

$\boldsymbol{a}_o$. Towards that, we first note that the power transmitted in the second phase by the relays is given by

$$\mathbb{E}\left[\boldsymbol{a}_o^\dagger \text{diag}\left(\boldsymbol{y}_r^*\right)\text{diag}\left(\boldsymbol{y}_r\right)\boldsymbol{a}_o\right]$$
$$= \boldsymbol{a}_o^\dagger \left(\text{diag}\left(\boldsymbol{h}_r^*\right)\text{diag}\left(\boldsymbol{h}_r\right)\bar{P} + \boldsymbol{I}_K\right)\boldsymbol{a}_o \triangleq \boldsymbol{a}_o^\dagger \boldsymbol{A}\boldsymbol{a}_o. \quad (42)$$

Next, we rewrite the constraint (38) slightly differently as

$$\boldsymbol{a}_o = \mathcal{P}^\perp(\text{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{g}_e)\boldsymbol{u}_a \triangleq \boldsymbol{F}\boldsymbol{u}_a \quad (43)$$

for some vector $\boldsymbol{u}_a \in \mathbb{C}^K$ to be designed. Next, we note that for the strong user, using (42) and (43), finding the optimal $\boldsymbol{u}_a$ is tantamount to solving the following problem (note that $\boldsymbol{F}$ is a Hermitian matrix):

$$\max_{\boldsymbol{u}_a} \quad \frac{\boldsymbol{u}_a^\dagger \boldsymbol{F}\boldsymbol{G}_{1,r}\boldsymbol{F}\boldsymbol{u}_a}{1 + \boldsymbol{u}_a^\dagger \boldsymbol{F}\boldsymbol{G}_1\boldsymbol{F}\boldsymbol{u}_a}$$
$$\text{s.t.} \quad \boldsymbol{u}_a^\dagger \boldsymbol{F}\boldsymbol{A}\boldsymbol{F}\boldsymbol{u}_a = P - \bar{P} \quad (44)$$

which can be equivalently rewritten as the following problem:

$$\max_{\boldsymbol{u}_a} \quad \frac{\boldsymbol{u}_a^\dagger \boldsymbol{F}\boldsymbol{G}_{1,r}\boldsymbol{F}\boldsymbol{u}_a}{\boldsymbol{u}_a^\dagger \boldsymbol{F}\left(\frac{1}{P-\bar{P}}\boldsymbol{A} + \boldsymbol{G}_1\right)\boldsymbol{F}\boldsymbol{u}_a} \quad (45)$$

whose solution is given by the leading *generalized* eigenvector [18] of the following matrix pencil:

$$\left(\boldsymbol{F}\boldsymbol{G}_{1,r}\boldsymbol{F} \ , \ \boldsymbol{F}\left(\frac{1}{P-\bar{P}}\boldsymbol{A} + \boldsymbol{G}_1\right)\boldsymbol{F}\right) \quad (46)$$

i.e., the generalized eigenvector corresponding to the largest generalized eigenvalue of the pencil. Let us denote such a vector by $\boldsymbol{u}_a^{(1)}$. Similarly, one can show that the optimal $\boldsymbol{u}_a$ for the weak user is given by the leading generalized eigenvector of the following matrix pencil:

$$\left(\boldsymbol{F}\boldsymbol{G}_{2,r}\boldsymbol{F} \ , \ \boldsymbol{F}\left(\frac{1}{P-\bar{P}}\boldsymbol{A} + \boldsymbol{G}_2 + \boldsymbol{G}_{2,r}\alpha\bar{P}\right)\boldsymbol{F}\right) \quad (47)$$

which we denote by $\boldsymbol{u}_a^{(2)}$. To satisfy the power constraint (42) and the orthogonality constraint (43), the corresponding $\boldsymbol{a}_o^{(j)}$, $j = 1, 2$, is given by

$$\boldsymbol{a}_o^{(j)} = \sqrt{\frac{P - \bar{P}}{\boldsymbol{u}_a^{(j)T}\boldsymbol{F}\boldsymbol{A}\boldsymbol{F}\boldsymbol{u}_a^{(j)}}}\boldsymbol{F}\boldsymbol{u}_a^{(j)}, \quad j = 1, 2. \quad (48)$$

Then, as in the decode-and-forward scheme, we propose choosing the optimal $\hat{\boldsymbol{a}}_o$ by the following convex combination:

$$\hat{\boldsymbol{a}}_o = \beta\boldsymbol{a}_o^{(1)} + (1 - \beta)\boldsymbol{a}_o^{(2)} \quad (49)$$

for some $0 \le \beta \le 1$ of choice. Given $\hat{\boldsymbol{a}}_o$, we substitute in (40) and (41) to get the achievable secrecy rates.

VI. NUMERICAL EVALUATIONS

In this section, we first discuss evaluating the optimal transmit power and the optimal power fraction for each of the proposed relaying schemes, such that the secrecy rate region is maximized. Specifically, we characterize the boundary of the secrecy rate region by solving the following problem:

$$\max_{\alpha, \bar{P}} \quad \mu r_{s,1}^n + (1 - \mu)r_{s,2}^n$$

$$\text{s.t.} \quad 0 \le \bar{P} \le P, \quad 0 \le \alpha \le 1 \quad (50)$$

for some $\mu \in [0, 1]$, and $n \in \{J, DF, AF\}$ corresponds to one of the proposed schemes. For the decode-and-forward scheme, we do an outer maximization over the decoding order (i), $i = 1, 2$ (see (21) and (22)). We use a line search algorithm to numerically solve the above problem. Note that the feasible set is bounded, which facilitates the convergence of the algorithm to an optimal point. We use $\beta = \mu$ in (28) and (49).

The physical layout we consider is a one-dimensional system, where the strong user, the weak user, and the eavesdropper are located at 30 meters, 40 meters, and 50 meters from the BS, respectively. We have $K = 5$ relays, and for simplicity we assume that they are all close enough to each other that they are approximately at the same distance of 15 meters from the BS. To emphasize the effect of distance on the channel gains, we use the following simplified channel model [12]: $h = \sqrt{1/l^\gamma}e^{j\theta}$, where h is the channel gain between two nodes, l is the distance between them, $\gamma = 3.5$ is the path loss exponent, and θ is a uniform random variable in $[0, 2\pi]$. We denote by l_e the distance from the BS to the eavesdropper. We set P to 30 dBm[4]. We run multiple iterations of the simulations and compute the average performance.

In Fig. 2, we plot the achievable secrecy rate regions of the proposed schemes. Solid lines represent the system parameters stated above, and dashed lines represent the case of $l_e = 20$ meters. We see that when $l_e = 50$ meters, cooperative jamming outperforms direct transmission and is in turn outperformed by both decode-and-forward and amplify-and-forward which perform relatively close to each other. With $l_e = 20$ meters, direct transmission achieves zero secrecy rates since the eavesdropper is closer to the BS than both users. However, strictly positive secrecy rates are achievable by all the relaying schemes. We also see that cooperative jamming performs best, since the relays are close to the eavesdropper and hence their jamming effect is quite powerful. For parts of the region, it even performs very close to decode-and-forward and amplify-and-forward for the $l_e = 50$ meters case.

Next, we show the effect of the number of relays on the achievable *secrecy sum rates* of the proposed schemes in Fig. 3. Again we observe that all relaying schemes achieve positive secrecy sum rates when $l_e = 20$ meters and that cooperative jamming performs best in this case. We also observe that amplify-and-forward is more sensitive than the other schemes to the number of relays.

Finally, we fix the users' distances and show the effect of the relays' distance from the BS (and hence the users) on the achievable secrecy sum rates in Fig. 4. For this case, we vary the relays' distance but still keep them closer to the BS than the legitimate users and the eavesdropper. The dashed lines in this case are when $l_e = 27$ meters. We see that only the cooperative jamming scheme's performance monotonically increases with the relays' distance, which is again attributed to the fact that the jamming effect is more powerful when the

---

[4]Note that the noise power is normalized in this paper, and hence P also represents the SNR.
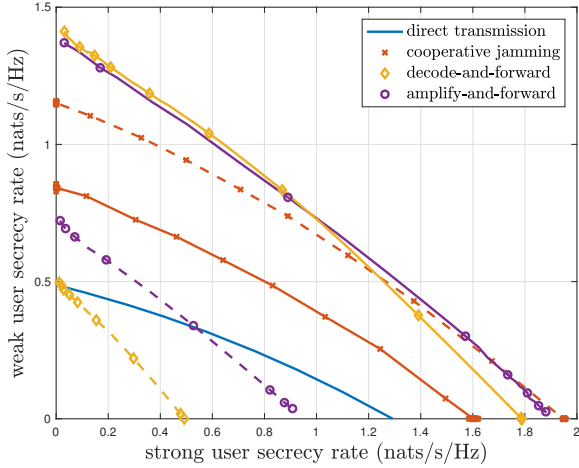
Fig. 2. Achievable secrecy rate regions of the proposed schemes. Solid lines are when $l_e = 50$ meters, and dashed lines are when $l_e = 20$ meters.
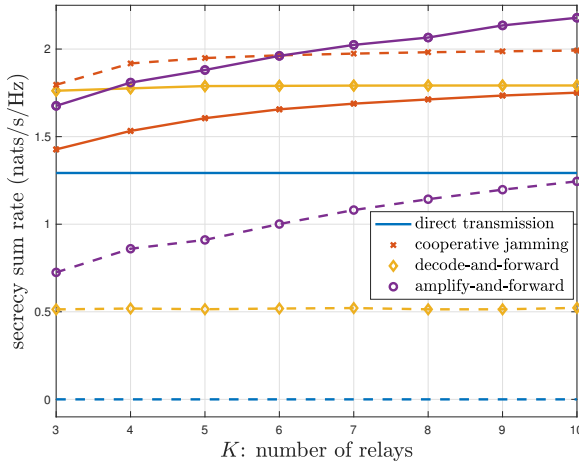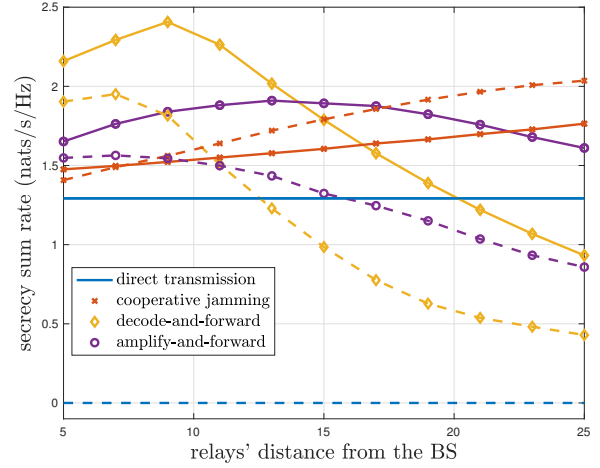

Fig. 4. Achievable secrecy sum rates vs. relays' distance from the BS. Solid lines are when $l_e = 50$ meters, and dashed lines are when $l_e = 27$ meters.

Fig. 3. Achievable secrecy sum rates vs. the number of relays. Solid lines are when $l_e = 50$ meters, and dashed lines are when $l_e = 20$ meters.

relays get closer to the eavesdropper.

VII. CONCLUSION

The security benefits of using trusted cooperative half duplex relays in a two-user SISO NOMA downlink system with an external eavesdropper have been studied under three relaying schemes: cooperative jamming, decode-and-forward, and amplify-and-forward. For each scheme, secure beamforming signals have been designed at the relays to maximize the achievable secrecy rate region. While the schemes improve the secrecy rate region, their performance varies depending on the eavesdropper's and relays' distances from the BS and also on the number of relays.

REFERENCES

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C.-L. I, and H. V. Poor. Application of non-orthogonal multiple access in LTE and 5G networks. *IEEE Commun. Mag.*, 55(2):185–191, February 2017.

[2] H. V. Poor and R. F. Schaefer. Wireless physical layer security. *Proc. National Academy of Sciences of USA*, 114(1):19–26, January 2017.

[3] Y. Zhang, H. M. Wang, Q. Yang, and Z. Ding. Secrecy sum rate maximization in non-orthogonal multiple access. *IEEE Commun. Lett.*, 20(5):930–933, May 2016.

[4] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Trans. Wireless Commun.*, 16(3):1656–1672, March 2017.

[5] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu, and M. Elkashlan. Uplink NOMA in large-scale systems: Coverage and physical layer security. Available Online: arXiv:1709.04693.

[6] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor. On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming. *IEEE Trans. Commun.*, 65(7):3151–3163, July 2017.

[7] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin. Secrecy sum rate optimization for downlink MIMO nonorthogonal multiple access systems. *IEEE Signal Process. Lett.*, 24(8):1113–1117, August 2017.

[8] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin. Secure beamforming in downlink MISO nonorthogonal multiple access systems. *IEEE Trans. Veh. Technol.*, 66(8):7563–7567, August 2017.

[9] M. Jiang, Y. Li, Q. Zhang, Q. Li, and J. Qin. Secure beamforming in downlink MIMO nonorthogonal multiple access networks. *IEEE Signal Process. Lett.*, 24(12):1852–1856, December 2017.

[10] H. Lei, J. Zhang, K. H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M. S. Alouini. On secure NOMA systems with transmit antenna selection schemes. *IEEE Access*, 5:17450–17464, September 2017.

[11] B. He, A. Liu, N. Yang, and V. K. N. Lau. On the design of secure non-orthogonal multiple access systems. *IEEE JSAC*, 35(10):2196–2206, October 2017.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.*, 58(3):1875–1888, March 2010.

[13] T. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 2006.

[14] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. *IEEE Trans. Inf. Theory*, 57(4):2083–2114, April 2011.

[15] B. Friedlander and B. Porat. Performance analysis of a null-steering algorithm based on direction of arrival estimation. *IEEE Trans. Signal Process.*, 37(4):461–466, April 1989.

[16] A. El Gamal and Y. H. Kim. *Network Information Theory*. Cambridge University Press, 2011.

[17] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[18] G. H. Golub and C. F. Van Loan. *Matrix Computations*. Johns Hopkins University Press, 2012.