Downlink Non-Orthogonal Multiple Access Systems With an Untrusted Relay

Ahmed Arafa[1], Wonjae Shin[2,1], Mojtaba Vaezi[3], 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 (SISO) non-orthogonal multiple access (NOMA) system in which a base station (BS) is communicating with two users is considered. An *untrusted* half-duplex relay node is available to assist with the BS's transmission. The BS uses superposition coding to transmit its messages, and the relay employs either a *compress-and-forward* or an *amplify-and-forward* scheme to communicate with the users. Two modes of operation are considered: *passive user* mode, and *active user* mode. In the passive user mode, the users receive data from both a direct link from the BS and the relay's forwarding link, and use that to decode their messages. In the active user mode, the users send a *cooperative jamming* signal simultaneously with the BS's transmission to confuse the relay. The focus is on half-duplex nodes, and hence the users cannot receive data from the BS's direct link in the active user mode while transmitting the cooperative jamming signal; they receive it only through the relay's forwarding link. For each mode, and under each relaying scheme, achievable secrecy rate regions are developed. Results show that the best relaying scheme and user mode depend on relative distances among the nodes, and on which part of the secrecy region the system is operating at.**

I. Introduction

NOMA techniques offer the promise of efficient utilization of resources for future mobile wireless networks, serving multiple users simultaneously per resource block, as opposed to conventional orthogonal multiple access techniques [1]. Employment of relay nodes is a natural choice in wireless communication systems to serve relatively distant users and enhance the rates of communication. However, such relay nodes may be *untrusted*, e.g., with lower security clearance relative to the end users, and hence transmission schemes should be designed such that the relays can only forward the data without revealing its actual contents. Physical layer security is a powerful, and provably unbreakable, tool to achieve such goal, as opposed to other security measures employed in higher layers of the communication protocol stack, see, e.g., [2] and the references therein. In this paper, we develop achievable secrecy rate regions for a two-user SISO NOMA system in the presence of an untrusted relay node.

Physical layer security in NOMA systems has been considered in the recent literature mainly through the lens of an external eavesdropper scenario, with the objective of characterizing/optimizing certain security measures, such as secrecy rates and secrecy outage probabilities, under both single and multiple antennas settings [3]–[11].

Information-theoretic analysis of communication systems with untrusted relay nodes are considered in [12]–[17]. References [12]–[14] consider the setting of deaf relays, i.e., relays that are ignorant of the source's transmitted signal, in the presence of external eavesdroppers, and develop achievable secrecy rates based on cooperative jamming and noise forwarding schemes. References [15] and [16] study a two-hop scenario with an untrusted relay (with no external eavesdroppers) and provide achievable secrecy rates for a single source-destination pair and for a multi-terminal setting, respectively, with the help of cooperative jamming signals from the destination(s). The general untrusted relay channel (also with no external eavesdropper) is considered in [17], where positive secrecy rates are shown achievable if the source-relay channel is orthogonal to the relay-destination channel via compress-and-forward scheme at the relay. For a summary of cooperative security works, see, e.g., [18] and the references therein.

In this work, we consider a downlink SISO NOMA system where a BS is communicating with two users in the presence of an untrusted relay node. All nodes are half-duplex, and communication takes place over two phases. In the first phase, the BS broadcasts its messages to both the users and the relay. In the second phase, the relay employs either *compress-and-forward* or *amplify-and-forward* to transmit its received data to the users. The users can either operate in *passive* or *active* modes. In the passive user mode, the users receive data through both the BS's direct link and the relay's forwarding link. In the active user mode, the users transmit a *cooperative jamming* signal, simultaneously with the BS's transmission during the first phase, to confuse the relay. Since we focus on half-duplex nodes, the users in the active mode cannot receive data through the BS's direct link while simultaneously transmitting the cooperative jamming signal, and receive it only through the relay's forwarding link. For both modes, and under both relaying schemes, we develop achievable secrecy rate regions based on superposition coding at the BS, under an overall system power constraint that is divided among the BS, the relay, and the users (if they are in the active mode). Results show that the developed schemes perform better than the direct approach of simply treating the relay as an external eavesdropper; they also show that the best relaying scheme and user mode depend on system parameters, in particular relative distances between the nodes, and on the system's operating point of the secrecy rate region.

This work was supported in part by the U.S. National Science Foundation under Grant CNS-1702808.

II. System Model

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

We denote the channel between the BS and the strong user (resp. weak user) by h_1 (resp. h_2), with[1] $|h_1|^2 > |h_2|^2$. 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 mean and unit variance, $\mathcal{CN}(0,1)$, 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 the 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, $\alpha \in [0,1]$ is the fraction of power allocated to the strong user, and $\bar{\alpha} \triangleq 1-\alpha$. Under such encoding and decoding schemes, we can achieve the following rates of this (degraded) Gaussian broadcast channel [19]:

$$r_1 = \log\left(1 + |h_1|^2 \alpha P\right), \tag{4}$$

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

An *untrusted* half-duplex relay node is available to assist with the BS's transmission. The relay is untrusted in the sense that it should be kept ignorant of the messages sent towards the users. However, it is assumed that the relay is *unmalicious* in the sense that it would not deviate from its transmission scheme, or attempt to hurt the users; it can only be curious enough to attempt to decode the users' messages. Let the received signal by the relay from the BS be given by

$$y_r = h_r x + n_r, \tag{6}$$

where h_r denotes the channel between the BS and the relay, and the noise term $n_r \sim \mathcal{CN}(0,1)$. One direct approach to deal with this untrusted relay situation is to simply treat it as an external eavesdropper and do not cooperate with it. This way, for a given α, the following secrecy rates are achievable for this multi-receiver wiretap channel [20, Theorem 5]:

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

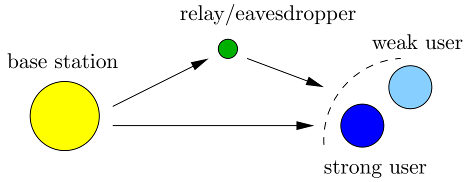

Fig. 1. Downlink NOMA system model with an untrusted relay node, and passive users.

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

where the subscript s, here and throughout the paper, is to denote secrecy rates, and $[x]^+ \triangleq \max\{x, 0\}$. Clearly, this leads to zero secrecy rates if the relay is closer to the BS than the users and has a relatively better channel, i.e., $|h_r|^2 > |h_1|^2$. However, it has been shown in [17] that positive secrecy rates can be achieved via *compress-and-forward* and *amplify-and-forward* relaying schemes, as opposed to treating the relay as an external eavesdropper, when the relay-to-users channel is orthogonal to the BS-to-relay channel, which is the case for instance if the relay is half-duplex as in this paper.

In the sequel, we extend the ideas of [17] to work in the context of NOMA, i.e., with multiple receivers, under two different modes of operation, namely, the *passive user* mode and the *active user* mode.

III. Passive User Mode

In the passive user mode, communication occurs over two phases. During the first phase, the BS broadcasts its messages to the users and to the relay. Then, the relay employs either a compress-and-forward or an amplify-and-forward scheme during the second phase to transmit its received message in the first phase towards the users, see Fig. 1. The received signals at the users during the second phase are given by

$$y_1^r = g_1 x_r + n_1^r, \tag{9}$$

$$y_2^r = g_2 x_r + n_2^r, \tag{10}$$

where x_r is the signal transmitted by the relay, g_j is the channel between the relay and user j, and the noise terms n_j^r, $j=1,2$, are i.i.d. $\sim \mathcal{CN}(0,1)$. The system's total power budget P is divided into $\bar{P} \leq P$ for the BS and $P - \bar{P}$ for the relay. We discuss the achievable secrecy rates under the two relaying schemes next.

A. Compress-and-Forward

Under the compress-and-forward scheme, the relay compresses its received signal y_r into another signal $\hat{y}_r \triangleq y_r + n_Q$, where n_Q is the quantization noise, and then encodes the quantized signal into its transmitted signal x_r. Following the results in [17, Theorem 3], setting $n_Q \sim \mathcal{CN}\left(0, \sigma_Q^2\right)$ and $x_r \sim \mathcal{CN}\left(0, P - \bar{P}\right)$, the achievable rates at the users under superposition coding are given by

$$\begin{aligned} r_1^{CF,P} &= I\left(x; h_1 x + n_1, h_r x + n_r + n_Q | s_2\right) \\ &= \log\left(1 + |h_1|^2 \alpha \bar{P} + \frac{|h_r|^2 \alpha \bar{P}}{1 + \sigma_Q^2}\right), \end{aligned} \tag{11}$$

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

$$r_2^{CF,P} = I\left(s_2; h_2 x + n_2, h_r x + n_r + n_Q\right)$$
$$= \log\left(1 + \frac{|h_2|^2\bar{\alpha}\bar{P}}{1+|h_2|^2\alpha\bar{P}} + \frac{|h_r|^2\bar{\alpha}\bar{P}}{1+|h_r|^2\alpha\bar{P}+\sigma_Q^2}\right), \quad (12)$$

where the superscript CF, P is to denote the compress-and-forward scheme under the passive user mode, and $I(\cdot;\cdot)$ denotes the mutual information measure [19]. Upon observing that the achievable rates in (11) and (12) are both decreasing in σ_Q^2. Such quantization noise power, however, should be designed to ensure decodability at both users [17, Theorem 3]. Omitting details for space limits, we set it to

$$\sigma_Q^2 = \min\left\{ \frac{\left(|h_r|^2 + |h_1|^2\right)\bar{P}+1}{|g_1|^2(P-\bar{P})(|h_1|^2\bar{P}+1)}, \frac{\left(|h_r|^2 + |h_2|^2\right)\bar{P}+1}{|g_2|^2(P-\bar{P})(|h_2|^2\bar{P}+1)} \right\}. \quad (13)$$

Hence, the achievable secrecy rates are given by

$$r_{s,1}^{CF,P} = \frac{1}{2}\left[r_1^{CF,P} - \log\left(1+|h_r|^2\alpha\bar{P}\right)\right]^+, \quad (14)$$
$$r_{s,2}^{CF,P} = \frac{1}{2}\left[r_2^{CF,P} - \log\left(1+\frac{|h_r|^2\bar{\alpha}\bar{P}}{1+|h_r|^2\alpha\bar{P}}\right)\right]^+, \quad (15)$$

where the extra $1/2$ term is due to sending the same message over two phases of equal durations.

B. *Amplify-and-Forward*

Under the amplify-and-forward scheme, the relay multiplies its received signal by a factor β and forwards it to the users. Hence, one can treat the overall system as a SIMO system from the users' viewpoint, and therefore the achievable rates at the users under superposition coding are given by

$$r_1^{AF,P} = \log\left(1+|h_1|^2\alpha\bar{P} + \frac{|g_1|^2\beta^2|h_r|^2\alpha\bar{P}}{1+|g_1|^2\beta^2}\right), \quad (16)$$
$$r_2^{AF,P} = \log\left(1+\frac{|h_2|^2\bar{\alpha}\bar{P}}{1+|h_2|^2\alpha\bar{P}} + \frac{|g_2|^2\beta^2|h_r|^2\bar{\alpha}\bar{P}}{1+|g_2|^2\beta^2\left(1+|h_r|^2\alpha\bar{P}\right)}\right), \quad (17)$$

where the superscript AF, P is to denote the amplify-and-forward scheme under the passive user mode, and the term β satisfies the following power constraint: $\beta^2 = \frac{P-\bar{P}}{1+|h_r|^2\bar{P}}$. Therefore, the achievable secrecy rates are given by

$$r_{s,1}^{AF,P} = \frac{1}{2}\left[r_1^{AF,P} - \log\left(1+|h_r|^2\alpha\bar{P}\right)\right]^+, \quad (18)$$
$$r_{s,2}^{AF,P} = \frac{1}{2}\left[r_2^{AF,P} - \log\left(1+\frac{|h_r|^2\bar{\alpha}\bar{P}}{1+|h_r|^2\alpha\bar{P}}\right)\right]^+. \quad (19)$$

IV. Active User Mode

In the active user mode, communication also occurs over two phases as in the passive user mode except that the users send a *cooperative jamming* signal during the first phase to confuse the relay, and hence the notation *active user*. Our focus is on half-duplex nodes, and therefore we assume that the users cannot receive the BS's signal during the first phase while they are sending the jamming signal; instead, they only rely on the signal received from the relay during the second (forwarding) phase to decode their messages. Thus, in effect, there is no direct link between the BS and the users in the active user mode, and the model converts to a two-hop network, see Fig. 2.

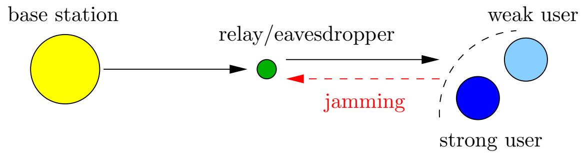

Fig. 2. Downlink NOMA system model with an untrusted relay node, and active users.

Let $\boldsymbol{J}z$ denote the jamming signal, with the beamfoming vector $\boldsymbol{J} \in \mathbb{C}^2$ and $z \sim \mathcal{CN}(0,1)$. Thus, the received signal at the relay during the first phase is now given by

$$y_r = h_r x + \boldsymbol{g}^\dagger \boldsymbol{J} z + n_r, \quad (20)$$

where $\boldsymbol{g} \triangleq [g_1 \; g_2]$. The system's total power budget in this case is divided into $\bar{P} \leq P$ for the BS, $P - \bar{P} - \delta$ for the relay, and $\delta \leq P - \bar{P}$ for the users. Note that the case of $\delta = 0$ is operationally equivalent to the users being passive, and hence the direct link from the BS to the users is reestablished. We therefore proceed with the assumption that $\delta > 0$. Otherwise, the users would stay silent for half of the communication session unnecessarily. Comparing the performance of passive and active modes is not straightforward though. For instance, as we show below, setting $\delta = 0$ in the rates achieved for active users, while mathematically approvable, does *not* give the same rates achieved by passive users. This is mainly because in the active user mode, the system becomes a two-hop network with no direct link from the BS to the users, unlike in the passive user mode. We discuss this in more detail and compare the performance of passive and active users in Section V.

In order to maximally diminish the relay's decoding ability, the beamforming vector is chosen as

$$\boldsymbol{J} = \frac{\boldsymbol{g}}{\|\boldsymbol{g}\|}\sqrt{\delta}. \quad (21)$$

The beamforming vector $\boldsymbol{J}$ is computed at the relay and then shared with the two users so that they compute their cooperative jamming signal. We discuss the achievable secrecy rates under the two relaying schemes, compress-and-forward and amplify-and-forward, next.

A. *Compress-and-Forward*

The compress-and-forward scheme with active users is similar to the scheme presented in Section III-A except that there is no direct link. In addition, the users subtract their jamming signal from their received signals from the relay before decoding. Hence, the achievable rates at the (active) users are given by

$$r_1^{CF,A} = \log\left(1+\frac{|h_r|^2\alpha\bar{P}}{1+\sigma_Q^2}\right), \quad (22)$$
$$r_2^{CF,A} = \log\left(1+\frac{|h_r|^2\bar{\alpha}\bar{P}}{1+|h_r|^2\alpha\bar{P}+\sigma_Q^2}\right), \quad (23)$$

where the superscript CF, A is to denote the compress-and-forward scheme under the active user mode, and the quantization noise power σ_Q^2 is now given by

$$\sigma_Q^2 = \min\left\{ \frac{\left(|h_r|^2 + |h_1|^2\right)\bar{P} + 1}{|g_1|^2(P - \bar{P} - \delta)(|h_1|^2\bar{P} + 1)}, \right. \left. \frac{\left(|h_r|^2 + |h_2|^2\right)\bar{P} + 1}{|g_2|^2(P - \bar{P} - \delta)(|h_2|^2\bar{P} + 1)} \right\}. \quad (24)$$

Therefore, the achievable secrecy rates are given by

$$r_{s,1}^{CF,A} = \frac{1}{2}\left[r_1^{CF,A} - \log\left(1 + \frac{|h_r|^2\alpha\bar{P}}{1 + \|\boldsymbol{g}\|^2\delta}\right)\right]^+, \quad (25)$$

$$r_{s,2}^{CF,A} = \frac{1}{2}\left[r_2^{CF,A} - \log\left(1 + \frac{|h_r|^2\bar{\alpha}\bar{P}}{1 + \|\boldsymbol{g}\|^2\delta + |h_r|^2\alpha\bar{P}}\right)\right]^+. \quad (26)$$

B. Amplify-and-Forward

Proceeding as above, the users subtract their jamming signal from their received signals from the relay before decoding. This can be done if the term β is known at the users, which is achieved by sharing the BS-to-relay channel gain h_r, along with the relay's transmit power, with them. Following the approach in Section III-B, the achievable rates at the (active) users under the amplify-and-forward scheme are given by

$$r_1^{AF,A} = \log\left(1 + \frac{|g_1|^2\beta^2|h_r|^2\alpha\bar{P}}{1 + |g_1|^2\beta^2}\right), \quad (27)$$

$$r_2^{AF,A} = \log\left(1 + \frac{|g_2|^2\beta^2|h_r|^2\bar{\alpha}\bar{P}}{1 + |g_2|^2\beta^2\left(1 + |h_r|^2\alpha\bar{P}\right)}\right), \quad (28)$$

where the term β now satisfies the following power constraint: $\beta^2 = \frac{P - \bar{P} - \delta}{1 + |h_r|^2\bar{P}}$. Thus, the achievable secrecy rates are

$$r_{s,1}^{AF,A} = \frac{1}{2}\left[r_1^{AF,A} - \log\left(1 + \frac{|h_r|^2\alpha\bar{P}}{1 + \|\boldsymbol{g}\|^2\delta}\right)\right]^+, \quad (29)$$

$$r_{s,2}^{AF,A} = \frac{1}{2}\left[r_2^{AF,A} - \log\left(1 + \frac{|h_r|^2\bar{\alpha}\bar{P}}{1 + \|\boldsymbol{g}\|^2\delta + |h_r|^2\alpha\bar{P}}\right)\right]^+. \quad (30)$$

V. Numerical Results

We now present some numerical examples. We characterize the boundary of the achievable secrecy rate region by solving:

$$\begin{aligned} \max_{\alpha, \bar{P}} \quad & \mu r_{s,1}^n + (1 - \mu) r_{s,2}^n \\ \text{s.t.} \quad & 0 \le \bar{P} \le P, \quad 0 \le \alpha \le 1, \end{aligned} \quad (31)$$

for some $\mu \in [0, 1]$, and the superscript n can be (CF, P), (AF, P), (CF, A), or (AF, A). For simplicity, when considering the active user mode, we set the users jamming signal power $\delta = \frac{P - \bar{P}}{2}$ and do not further optimize it. 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.

The physical layout that we consider is a simple one-dimensional system, where the strong user, the weak user, and the relay are located at 40, 50, and 35 meters away from the BS, respectively. To emphasize the effect of distance on the channel gains, we use the following simplified channel model: $h = \sqrt{1/l^\gamma}e^{j\theta}$, 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 $[0, 2\pi]$. Let l_r denote the distance from the BS to the relay. We set P to 30 dBm. We run multiple iterations of the simulations and compute the average performance.

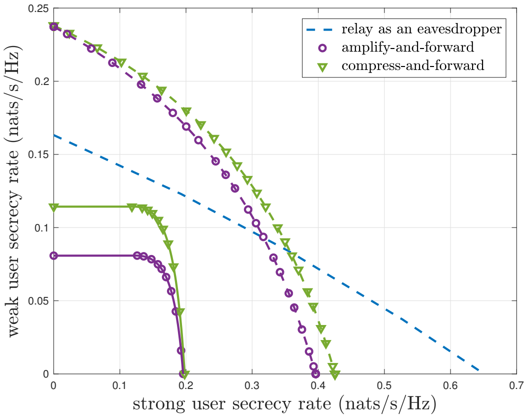

Fig. 3. Achievable secrecy rate region with *passive* users. Solid lines are when $l_r = 35$ meters; dashed lines are when $l_r = 55$ meters.

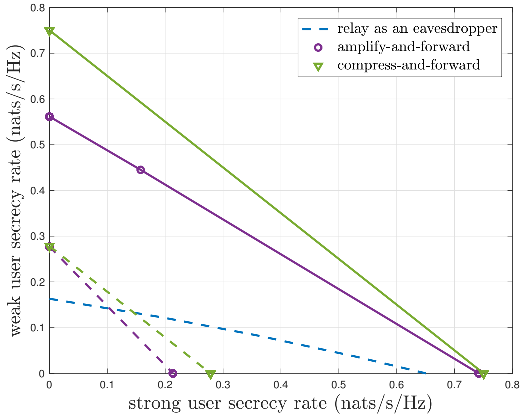

Fig. 4. Achievable secrecy rate region with *active* users. Solid lines are when $l_r = 35$ meters; dashed lines are when $l_r = 55$ meters.

In Fig. 3, we plot the achievable secrecy rate regions of the proposed schemes under the passive user mode, along with the direct transmission scheme in which the relay is treated as an eavesdropper. We also plot the results for the case when $l_r = 55$. When $l_r = 35$, direct transmission achieves zero secrecy rates since the relay is closer to the BS than the users, while the two proposed schemes achieve strictly positive secrecy rates. When $l_r = 55$, the proposed schemes still outperform direct transmission for some parts of the region, showing the benefit of using the untrusted relay even if it is relatively further away from the BS. In both cases compress-and-forward completely outperforms amplify-and-forward.

In Fig. 4, we plot the achievable secrecy rate regions of the proposed schemes under the active user mode. Similar conclusions follow as in the passive user mode, yet with the following striking difference: the achievable rates when the

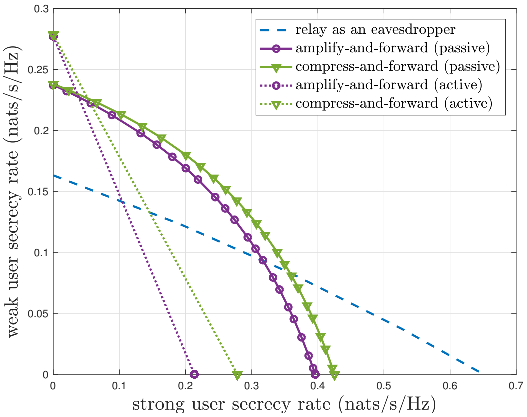

Fig. 5. Achievable secrecy rate region when $l_r = 55$ meters. Solid lines represent the passive user mode; dotted lines represent the active user mode.

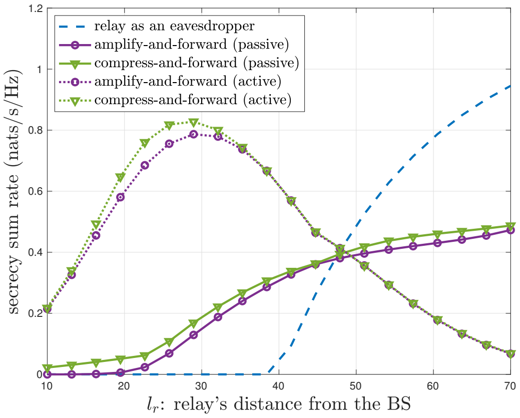

Fig. 6. Achievable secrecy sum rate vs. relay's distance from BS. Solid lines represent the passive user mode; dotted lines represent the active user mode.

untrusted relay is further away from the BS are actually lower than those achieved when it is closer to the BS. The main reason behind this is that in the active user mode the users rely completely on the relay to receive their messages during the second phase since they cannot receive while sending the jamming signal during the first one. Therefore, the further the relay, the worse the BS-to-relay channel and the lower its ability to forward the messages become. This observation raises a question on whether the users being active is worse than them being passive when the untrusted relay is relatively further away from the BS. We elaborate on this point in Figs. 5 and 6. In Fig. 5, we plot the secrecy rate region achieved under both the passive user and the active user modes when $l_r = 55$. We see that the passive user mode outperforms the active user mode almost entirely, and that it is still better than direct transmission in almost half of the region. In Fig. 6, we plot the achievable secrecy sum rate versus the relay's distance from the BS. We see that direct transmission starts achieving non-zero rate only after l_r grows above 40, which is the strong user's distance from the BS. We also see that there exists an optimal l_r value, beyond which the active user mode's performance starts to degrade. Finally, we see that there exists a threshold l_r value, after which the passive user mode beats the active user mode. We note that for $l_r = 55$, although direct transmission achieves higher secrecy sum rate than both passive and active user modes, it is still not entirely preferable, since we see from Fig. 5 that both modes beat direct transmission for higher values of the weak user's secrecy rate. Hence, in conclusion, the best relaying scheme depends on relay's distance from BS, and on which part of the secrecy region the system is operating at.

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 J. Sel. Areas Commun.*, 35(10):2196–2206, October 2017.

[12] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, September 2008.

[13] R. Bassily and S. Ulukus. Deaf cooperation and relay selection strategies for secure communication in multiple relay networks. *IEEE Trans. Signal Process.*, 61(6):1544–1554, March 2013.

[14] R. Bassily and S. Ulukus. Deaf cooperation for secrecy with multiple antennas at the helper. *IEEE Trans. Inf. Forensics Security*, 7(6):1855–1864, December 2012.

[15] X. He and A. Yener. Two-hop secure communication using an untrusted relay: A case for cooperative jamming. In *Proc. IEEE Globecom*, December 2008.

[16] A. Zewail and A. Yener. Multi-terminal two-hop untrusted-relay networks with hierarchical security guarantees. *IEEE Trans. Inf. Forensics Security*, 12(9):2052–2066, September 2017.

[17] X. He and A. Yener. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Trans. Inf. Theory*, 56(8):3807–3827, August 2010.

[18] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener. Cooperative security at the physical layer: A summary of recent advances. *IEEE Signal Process. Mag.*, 30(5):16–28, September 2013.

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

[20] 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.