Abstract—In this paper, we investigate an artificial-noise (AN) aided secure transmission for non-orthogonal multiple access (NOMA) full-duplex (FD) relay network. We propose a novel joint NOMA and AN-aided full-duplex relay (NOMA-ANFDR) scheme to enhance the physical security. In this scheme, the optimal power allocation between the information and the AN signal is determined such that the capacity of the two end-to-end (i.e., two source-relay-destination pairs) channel are maximized to ensure the highest quality of cooperative transmission. To fully examine the benefits of the NOMA-ANFDR scheme, we derive a new closed-form expression for the secrecy outage probability. We show that the NOMA-ANFDR scheme significantly outperforms the joint NOMA and AN in half-duplex relay (NOMA-ANHDR) scheme as well as the NOMA-HDR scheme in terms of minimum secrecy outage probability and effect secrecy throughout. This result indicates that adopting the joint of FD and AN technique at relays can effectively enhance the physical layer secrecy performance in the NOMA cooperative network.

I. INTRODUCTION

Recently, non-orthogonal multiple access (NOMA) has received enormous interests since it can significantly boost the system spectral efficiency [1]. Different from the conventional orthogonal multiple access methods such as frequency division multiple access, time division orthogonal multiple access, and code division multiple access, NOMA allows multiple users to share the same resource block (i.e., time/frequency/code), in which successive interference cancellation (SIC) has to be performed at one receiver to suppress the interference caused by other users’ information.

In [2], cooperative NOMA with maximum ratio combining was studied to enhance the spatial diversity. In [3], different relay selection strategies were proposed and analyzed in cooperative NOMA systems. In [4], outage probability and ergodic sum capacity were investigated in a NOMA system with coordinated direct and relay transmission. In [5], two source-destination user pairs sharing a common half-duplex relay was investigated in NOMA cooperative system. It is noted that cooperative NOMA introduced in [2–5] all adopt half-duplex cooperative relay mode. Meanwhile, the security of wireless communication is a pivotal issue that needs to be addressed in wireless networks. As a complimentary approach to the traditional cryptographic techniques, physical layer security has been recognized as a key solution to safeguard wireless data transmissions and thus attracted numerous research interests [6]. In the context of physical layer security, many technologies, such as artificial-noise (AN)-aided transmission, full-duplex techniques, and cooperative relay transmission, have been proposed to enhance the secrecy performance of wireless communications [7–13]. Specially, Generating AN at the legitimate transmitter is proposed to be an effective technique to confound the eavesdropper [8–12]. Cooperative full-duplex relay has also been proved as an effective way to improve the system security [9]. In [7], a physical layer security based on AN-aided strategy was first considered in relay networks, which can largely improve the physical-layer security. Motivated by the benefits of relay and AN assistance, many researchers have investigated various secure transmission strategies, such as cooperative beamforming (CB) [8] and cooperative jamming (CJ) [9].

Although physical layer security has been well studied in many scenarios, the design of secrecy transmission for NOMA cooperative is still not clear. The aim of this work is to examine the secure performance of NOMA protocol in cooperative networks. To answer this important question, we focus on a similar scenario considered in [5]. However, the authors did not consider the existence of eavesdropping users. Furthermore, in order to improve the security of the systems, AN-aided and full-duplex methods are applied in this communication scenario.

In this work, we exploit the use of AN-aided and full-duplex (FD) strategies at relay node to enhance the secrecy in NOMA cooperative networks. Specifically, we propose a novel joint NOMA and AN-aided full-duplex relay (NOMA-ANFDR) scheme. In this scheme, the optimal power allocation between the information and the AN signal is determined such that the capacity of the two end-to-end (i.e., two source-relay-destination pairs) channel are maximized to ensure the highest quality of cooperative transmission. To disclose the benefits of the NOMA-ANFDR scheme relative to the joint NOMA and AN-aided half-duplex relay scheme (NOMA-
ANFDR), we derive a new closed-form expression for the secrecy outage probability of the NOMA-ANFDR scheme. We also derive the secrecy outage probability of the NOMA-ANHDR scheme as a benchmark. Our analysis demonstrates that the NOMA-ANFDR scheme significantly outperforms the NOMA-ANHDR scheme by achieving a lower secrecy outage probability and a higher effect secrecy throughout when the self-interference at the FD relay can be reasonably suppressed. Furthermore, we also compare the AN-aided schemes (i.e., the NOMA-ANFDR and NOMA-ANHDR schemes) with joint NOMA and half-duplex relay scheme (NOMA-FDR). Our analysis demonstrates that the AN-aided schemes perform significantly better than the NOMA-HDR scheme.

II. PROPOSED NOMA-ANFDR SCHEME IN A COMMON FULL-DUPLEX-DF-RELAY NETWORK

We consider a secure cooperative relay network, as illustrated in Fig. 1, in which two source-destination pairs $S_1 - D_1$ and $S_2 - D_2$ share a common FD decode-and-forward (DF) relay $R$. All nodes in networks are equipped with a single antenna and operate in the full-duplex DF mode. We assume that $K$ eavesdroppers (E) exists in this network and overhears the transmission from the relay. Similar to [5], we also assume that the direct links from $S$ to $D$ and $E$ are not available due to the strong path-loss and attenuation between them. In this case, both $S_1$ and $S_2$ rely on $R$ to communicate simultaneously with their corresponding receivers $D_1$ and $D_2$, respectively. This assumption can be justified in case of urban areas where nodes are placed far apart, and is also in line with previous researches such as [3, 5].

In this work, we assume that all channels experience block Rayleigh fading such that the channels remain constant over one block but vary independently from one block to another [9], and we denote $f_{S_1,R} \sim \mathcal{CN}(0, d_{R}^{-n_R})$, $f_{S_2,R} \sim \mathcal{CN}(0, d_{R}^{-n_R})$, $h_{R,D_1} \sim \mathcal{CN}(0, d_{R}^{-n_D})$, $h_{R,D_2} \sim \mathcal{CN}(0, d_{R}^{-n_E})$, and $l_{R,E_k} \sim \mathcal{CN}(0, d_{R}^{-n_E})$ as the channel coefficients of the $S_1 - R$, $S_2 - R$, $R - D_1$, $R - D_2$, and $R - E_k$ links, respectively. We denote $P_S$ and $P_R$ as the transmit power at $S$ and $R$, respectively. We then denote that $n_R \sim \mathcal{CN}(0, \sigma_R^2)$, $n_D \sim \mathcal{CN}(0, \sigma_D^2)$, and $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ as the complex additive white Gaussian noise components at $R$, $D$, and $E$, respectively. Where $v$ is the path loss exponent and $d$ represents the distance in meters. In our considered network, it is anticipated that $|f_{S_1,R}| > |f_{S_2,R}|$ and $|d_{R,D_1}| > |d_{R,D_2}|$ because it is assumed that $d_{R,D_1} < d_{R,D_2}$ and $d_{R,D_2} < d_{R,D_1}$.

A. Information Received and Decoded on Relay

We assumed that, at the $n$-th time slot, both $S_1$ and $S_2$ simultaneously transmit symbols $x_1[n]$ and $x_2[n]$ with powers $\alpha_1 P_S$ and $\alpha_2 P_S$ to the relay, respectively, where $P_S$ is the total transmit power constraint, $\alpha_1$ and $\alpha_2$ denote power allocation coefficients, such that $\alpha_1 + \alpha_2 = 1$ and $\alpha_1 > \alpha_2$. It is assumed that $S_1$ and $S_2$ have some sort of cooperation and based on that, power is distributed between them to meet the total transmission power requirement. Note that the total transmit power requirement is essential for many practical scenarios [5, 15]. Similar to [5, 15], uplink NOMA method is used, the relay first decodes the better source symbol $x_1[n]$ by treating the symbol $x_2[n]$ of worse source as noise. We consider a FD relay in this communication scenario, and also assume that the relay transmit symbols $x_1[n]$ and $x_2[n]$ with powers $\alpha_3 P_R$ and $\alpha_4 P_R$ to $D_1$ and $D_2$, respectively, where $P_R$ is the total transmit power at relay. Then, the relay performs SIC to obtain symbol $x_2[n]$. Thus, the received signal-to-interference-plus-noise ratio (SINR) for symbol $x_1[n]$ and signal-to-plus-noise (SNR) for symbol $x_2[n]$ at the relay are given by

$$\gamma_{x_1} = \frac{\alpha_1 P_S |f_{S_1,R}|^2}{\alpha_2 P_S |f_{S_2,R}|^2 + P_R |h_{R,R}|^2 + \sigma_R^2}$$

and

$$\gamma_{x_2} = \frac{\alpha_3 P_R |f_{S_1,R}|^2}{P_R |h_{R,R}|^2 + \sigma_R^2}$$

respectively, where $\rho_S = \frac{P_S}{\sigma_R}$ and $\rho_{RR} = \frac{P_R}{\sigma_R}$, $h_{R,R} \sim \mathcal{CN}(0, \lambda_{RR})$ denotes channel coefficient for the relay self-interference channel. It is noted that the self-interference can be significantly suppressed so that $h_{R,R}$ can be regarded as an independent Rayleigh distributed variable [9].

B. Information Received and Decoded on Destinations

Recalling to the downlink NOMA in [5, 14], in which a superimposed composite signal are regenerated and transmitted. In our considered network, in order to improve the security of information transmission, similar to [8, 12], we proposed the use of so-called artificial noise aided secure transmission in the relay. As such, by adopting the superposition code, the transmitted signal at the relay is given by

$$S[n] = \sqrt{\alpha_3 P_R x_1[n]} + \sqrt{\alpha_4 P_R x_2[n]} + \sqrt{\alpha_5 P_R x_a[n]}$$

where $x_1[n]$ and $x_2[n]$ are the regenerated data symbols at during $n$-th time slot, $x_a$ is an artificial noise used to defend against eavesdropping, and $\alpha_5$ denote power allocation coefficient for artificial noise, such that $\alpha_3 + \alpha_4 + \alpha_5 = 1$ and $\alpha_3 > \alpha_4$. In this paper, we assume that the artificial noise transmitted by the relay is generated from a pseudo random sequence, which is known to the legitimate receivers (i.e., $R$, $D_1$, $D_2$).
\[ D_1 \text{ and } D_2 \) and remains unknown to the eavesdroppers [8, 12]. Furthermore, according to NOMA protocol, \( D_1 \) decodes own symbol \( x_1[n] \) by treating \( x_2[n] \) as noise. Therefore, the received SINR at \( D_1 \) for symbols \( x_1[n] \) is given as

\[
\gamma_{x_1}^d = \frac{\alpha_3 P_R |h_{R, D_1}|^2}{\alpha_4 P_R |h_{R, D_2}|^2 + \sigma_D^2} = \frac{\alpha_3 \rho_R |h_{R, D_1}|^2}{\alpha_4 P_R |h_{R, D_2}|^2 + 1},
\]

(4)

where \( \rho_R = \frac{P_R}{\sigma_D^2} \). On the other hand, according to NOMA protocol, the destination node with the stronger channel condition (i.e., \( D_2 \)) needs to firstly detect its partner’s information (i.e., \( D_1 \)) and then to obtain own information \( x_2 \) using SIC. Thus, the received SINR for \( x_1 \) and SNR for \( x_2 \) at \( D_2 \) are respectively given by

\[
\gamma_{x_1 \rightarrow x_2}^d = \frac{\alpha_3 P_R |h_{R, D_2}|^2}{\alpha_4 P_R |h_{R, D_2}|^2 + \sigma_D^2} = \frac{\alpha_3 \rho_R |h_{R, D_2}|^2}{\alpha_4 P_R |h_{R, D_2}|^2 + 1},
\]

(5)

and

\[
\gamma_{x_2}^d = \frac{\alpha_3 \rho_R |h_{R, D_2}|^2}{\sigma_D^2} = \frac{\alpha_4 P_R |h_{R, D_2}|^2}{\alpha_4 P_R |h_{R, D_2}|^2 + \sigma_D^2},
\]

(6)

where \( x_1 \rightarrow x_2 \) denotes the SINR required at \( D_2 \) to decode symbol \( x_1 \).

On the other hand, for eavesdroppers, following the similar assumption, we consider the worst-case scenario of large-scale networks in which eavesdroppers are assumed to have strong detection abilities and distinguished legal data stream from the relay [14]. Therefore, the instantaneous SINR for detecting the legal information of \( x_1[n] \) and \( x_2[n] \) at the most detrimental eavesdropper can be expressed as follows:

\[
\gamma_{E_i} = \max_{k=1, \cdots, K} \frac{\alpha_i P_R |l_{R, E_k}|^2}{\alpha_i \rho_E |l_{R, E_k}|^2 + \sigma_E^2} = \max_{k=1, \cdots, K} \frac{\alpha_i \rho_E |l_{R, E_k}|^2}{\alpha_i \rho_E |l_{R, E_k}|^2 + \sigma_E^2},
\]

(7)

where \( i \in \{3, 4\} \), \( \rho_E = \frac{P_R}{\sigma_E^2} \) is the transmit SINR, \( \sigma_E^2 \) is the variance of AWGN at eavesdroppers.

### III. New Channel Statistics

In this section, we derive several new channel statistics for destinations and eavesdroppers, which will be used to derive the secrecy outage probability in the next section.

**Theorem 1:** Conditioned on the two source-destination pairs \( S_1 - D_1 \) and \( S_2 - D_2 \) share a common DF relay in considered NOMA networks and the relay using the AS to confuse eavesdroppers, the PDF of the most detrimental eavesdropper \( \gamma_{E_i} \) is given by (8)

\[
f_{\gamma_{E_i}}(x) = \left\{ \begin{array}{ll}
\frac{(k+1) x (k+1) e^{-\frac{(k+1) x}{\sigma_E^2 (\alpha - \alpha_3) x}}}{{k^k} e^{-\frac{(k+1) x}{\sigma_E^2 (\alpha - \alpha_3) x}}}, & \text{if } x \leq \frac{\alpha_3}{\alpha_5}, \\
0, & \text{if } x > \frac{\alpha_3}{\alpha_5},
\end{array} \right.
\]

(8)

where \( \pi_{RE} = \rho_{RD}^{-1} \).

**Proof:** From (7), and let \( X_k = \frac{\alpha_i \rho_E |l_{R, E_k}|^2}{\alpha_i \rho_E |l_{R, E_k}|^2 + 1} = \frac{\alpha_i X}{\alpha_5 X + 1} \), we can obtain the CDF of \( X_k \) as

\[
F_{X_k}(x) = \Pr\left( \frac{\alpha_i X}{\alpha_5 X + 1} < x \right) = \Pr(X < \frac{x}{\alpha_5}, \frac{x}{\alpha_5} x - \alpha_5 x)
\]

(9)

and we can obtain the PDF of \( X_k \) as

\[
f_{X_k}(x) = \left\{ \begin{array}{ll}
\frac{\alpha_i \rho_{RE} x}{\pi_{RE} (\alpha - \alpha_3) x^2} e^{-\frac{x}{\pi_{RE} (\alpha - \alpha_3) x}}, & \text{if } x < \frac{\alpha_3}{\alpha_5}, \\
0, & \text{if } x > \frac{\alpha_3}{\alpha_5}.
\end{array} \right.
\]

(10)

We further obtain the CDF of \( \gamma_{E_i} \) as follows

\[
F_{\gamma_{E_i}}(x) = \Pr(\gamma_{E_i} < x) = \Pr(\max_{k=1, \cdots, K} X_k < x) = F_{X_k}(x)^K.
\]

(11)

Based on (9), (10), (11), and performing some mathematical manipulations, we obtain (8), which completes the proof of Theorem 1.

**Theorem 2:** Considered on the two source-destination pairs \( S_1 - D_1 \) and \( S_2 - D_2 \) share a common DF relay in considered NOMA networks, the cumulative distribution function (CDF) of SINR (SNR) for symbol \( x_1 \) is given by (12)

\[
F_{X_{S_1 D_1}}^1(x) = \left\{ \begin{array}{ll}
1 - \frac{e^{-\frac{\pi_{S_1 R}^2}{\rho_{S_1 R}}}}{\pi_{S_1 R}}, & \text{if } x \leq \frac{\alpha_3}{\alpha_5}, \\
\frac{\pi_{S_1 R}^2}{\rho_{S_1 R}^2}, & \text{if } x > \frac{\alpha_3}{\alpha_5}.
\end{array} \right.
\]

(12)

where \( \pi_{S_1 R} = \rho_{S_1 R}^{-1} \), \( \pi_{S_2 R} = \rho_{S_2 R}^{-1} \), \( \pi_{RD_1} = \rho_{RD_1}^{-1} \), \( \pi_{RD_2} = \rho_{RD_2}^{-1} \), and \( \pi_{RR} = \rho_{RR}^{-1} \).

**Proof:** By using (1), (4), and (5), the achievable SINR(SNR) associated with symbol \( x_1 \) is given by

\[
\rho_{S_1 D_1}(x_1) = \min\{\gamma^d_{x_11}, \gamma^d_{x_12}, \gamma^d_{x_1 \rightarrow x_2}\}. \quad (13)
\]

Recall (1), and let \( Y_1 = |f_{S_1 R}|^2, Y_2 = |f_{S_2 R}|^2, \) and \( Y_3 = |l_{R, R}|^2 \), \( \gamma_{x_1} \) can be reexpressed as \( \gamma_{y_1} = \alpha_2 \rho_{S_1 R} Y_1 + \alpha_2 \rho_{S_2 R} Y_2 + \frac{\alpha_5}{\alpha_5} \rho_{S_1 R} Y_3 \). We also assume \( \gamma_{y_1} = \alpha_2 \rho_{S_1 R} Y_1 + \frac{\alpha_5}{\alpha_5} \rho_{S_1 R} Y_3 \). We can easily obtain the PDF of \( x_4 \) as follows:

\[
f_{Y_4}(y) = c_1 e^{-\frac{\pi_{S_1 R} y}{\rho_{S_1 R}} + \frac{\pi_{S_1 R} y}{\rho_{S_1 R}}}.
\]

(14)

We further reexpress (1) as \( X_1 = \frac{\alpha_2 \rho_{S_1 R} Y_1}{\alpha_4 \rho_{S_1 R}^2 + 1} \), and the CDF of \( X_1 \) can be computed by

\[
F_{X_1}(x) = \Pr\{X_1 < x\} = \Pr\left(\frac{\alpha_2 \rho_{S_1 R} Y_1}{\alpha_4 \rho_{S_1 R}^2 + 1} \right) < x
\]

(15)

\[
= \int_0^\infty [1 - e^{-\frac{\pi_{S_1 R} y}{\rho_{S_1 R}}}] f_{Y_4}(y) dy.
\]

On the other hand, we let \( X_2 = \gamma_{x_1 \rightarrow x_2}^d = \frac{\alpha_3 \rho_R |l_{R, D_1}|^2}{\alpha_4 P_R |l_{R, D_2}|^2 + 1} \). Similar to the analysis in

Authorized licensed use limited to: UNSW Library. Downloaded on August 27,2021 at 12:36:56 UTC from IEEE Xplore. Restrictions apply.
Theorem 1, we can obtain the CDFs of $Y_2$ and $Y_3$ as follows:

$$F_{X_2}(x) = \begin{cases} 1 - e^{-\frac{x}{\pi R_{S_1}^2}}, & x \leq \frac{\alpha_3}{\alpha_4} \\ 1, & x > \frac{\alpha_3}{\alpha_4} \end{cases}$$  \(16\)

and

$$F_{X_3}(x) = \begin{cases} 1 - e^{-\frac{x}{\pi R_{S_2}^2}}, & x \leq \frac{\alpha_3}{\alpha_4} \\ 1, & x > \frac{\alpha_3}{\alpha_4} \end{cases}$$  \(17\)

According to (13), the CDF of $F_{X}^{S_1 D_1}(x)$ can be expressed as

$$F_{X}^{S_1 D_1}(x) = 1 - (1 - F_{X_1}(x))(1 - F_{X_2}(x))(1 - F_{X_3}(x)).$$  \(18\)

Substituting (14), (15), (16), and (17) into (18), with some mathematical manipulations, we obtain (12), which completes the proof of Theorem 2.

**Theorem 3:** Conditioned on the two source-destination pairs $S_1 - D_1$ and $S_2 - D_2$ share a common DF relay in the NOMA networks, the CDF of SNR of $S_2 - D_2$ link is given by

$$F_{X}^{S_2 D_2}(x) = 1 - \frac{\alpha_2 \pi S_2 R e^{-\gamma_{S_2 D_2} x}}{\alpha_2 \pi S_2 R + \pi R_{D_2} x}.$$  \(19\)

**Proof:** By using (2) and (6), the achievable SINR (SNR) associated with symbol $x_1$ is given by

$$\rho_{S_2 D_2}(x_2) = \min\{\gamma_{S_2 D_1}, \gamma_{S_2 D_2}\}.$$  \(20\)

Following similar arguments as that of Theorem 2 for the CDF of (SNR) for symbol $x_1$, we obtain (19), which completes the proof of Theorem 3.

**IV. SECRECY OUTAGE PROBABILITY AND EFFECT SECRECY THROUGHOUT ANALYSIS**

In this paper, the secrecy outage probability (SOP) and effect secrecy throughout (EST) are used as a secrecy performance metric. Additionally, the secrecy capacity of the $S_1 - D_1$ and $S_2 - D_2$ can be expressed as

$$C_{S_1 D_1} = (\log_2(1 + \rho_{S_1 D_1}) - \log_2(1 + \gamma_{E_3}))^+,$$  \(21\)

and

$$C_{S_2 D_2} = (\log_2(1 + \rho_{S_2 D_2}) - \log_2(1 + \gamma_{E_4}))^+,$$  \(22\)

respectively, where $(x)^+ = \max\{x, 0\}$.

**A. Exact Secrecy Outage Probability**

Given the secrecy information rate $R_1$ and $R_2$ for the $S_1 - D_1$ and $S_2 - D_2$, a secrecy outage is declared when the instantaneous secrecy capacity drops below $R_1$ and $R_2$, respectively. Based on (21), the SOP for $S_1 - D_1$ is given by

$$P_{S_1 D_1}(R_1) = \Pr\{C_{S_1 D_1} < R_1\} = \Pr\{\rho_{S_1 D_1} < 2^{-R_1} \gamma_{E_3} - 1\} = \int_0^\infty F_{X}^{S_1 D_1}(2^{-R_1} x) (1 - 1) f_{\gamma_{E_3}}(x) dx.$$  \(23\)

Based on (12) and (8), and using the assumption $\alpha_3 > \alpha_4$ in Section II, we obtain $P_{S_1 D_1}(R_1)$ as (24), shown on the top of next page, where $\theta(x) = \frac{2^{R_1} + 2^{-R_1} - 1}{\alpha_1 \pi S_1 R}$, and $\xi = \min((\frac{\alpha_3}{\alpha_4} + 1) 2^{-R_1} - 1, (\frac{\alpha_3}{\alpha_4} + 1) 2^{-R_1} - 1)$. Similarly, for the $S_2 - D_2$ user, based on (22), the SOP is given by

$$P_{S_2 D_2}(R_2) = \Pr\{C_{S_2 D_2} < R_2\} = \Pr\{\rho_{S_2 D_2} < 2^{-R_2} \gamma_{E_4} - 1\} = \int_0^\infty F_{X}^{S_2 D_2}(2^{-R_2} x) (1 - 1) f_{\gamma_{E_4}}(x) dx.$$  \(25\)

Substituting (8) and (19) into (25), we can obtain the expression of SOP of the $S_2 - D_2$ user as (26) on the second top page. Though the analysis on information decoded for $S_1 - D_1$ and $S_2 - D_2$ user pairs in Section II, we find the secrecy outage occur of the $S_1 - D_1$ user and $S_2 - D_2$ user are independent. In other words, the SOP of the $S_1 - D_1$ user pair has no effect on that of $S_2 - D_2$ user pair and vice versa. As such, the SOP of the proposed NOMA-ANFDR scheme for the considered networks can be expressed as (14)

$$P_{\text{out}\text{NOMA-ANFDR}} = 1 - (1 - P_{S_1 D_1})(1 - P_{S_2 D_2}).$$  \(27\)

Following a similar procedure to derive the SOP of the proposed NOMA-ANFDR scheme, we can obtain SOP of the NOMA-ANHDR scheme, which is used as a baseline to compare with the proposed NOMA-ANFDR scheme. Specifically, the SOP of the NOMA-ANHDR scheme is given by

$$P_{\text{out}\text{NOMA-ANHDR}} = 1 - K^2 \sum_{k_1=0}^{K-1} \sum_{k_2=0}^{K-1} (-1)^{k_1+k_2} \left(\begin{array}{c} K-1 \\ k_1 \end{array}\right) \left(\begin{array}{c} K-1 \\ k_2 \end{array}\right) \tau_1 \alpha_3 \alpha_4 \frac{\pi R_{E}}{\pi R_{E}} \times \varpi(\xi) \int_0^{\frac{\alpha_3}{\alpha_4} e^{-\frac{x}{2^R_2 R^2} + \frac{x}{\pi R_{S_1} R^2} + \frac{x}{\pi R_{E} R^2} \xi} dx,$$  \(28\)

where

$$\varpi(\xi) = \int_0^{\frac{\alpha_3}{\alpha_4} \frac{\pi R_{S_1} R^2}{\pi R_{S_1} R^2} - \frac{\pi R_{S_1} R^2}{\pi R_{S_1} R^2} \xi} dx,$$  \(29\)

$$\xi = \min\{\frac{\alpha_3}{\alpha_4} + 1\} 2^{-R_1} - 1, \frac{\alpha_3}{\alpha_4} + 1\} 2^{-R_1} - 1\},$$  \(30\)

$$\Phi(x) = 1 + \frac{\alpha_3 \pi S_1 R}{\alpha_3 \pi S_1 R} (2^{R_1} (1 - 1)) e^{-\frac{2^{R_1} x}{\pi R_{S_1} R^2}},$$  \(31\)

and

$$\tau_1 = e^{-\frac{1}{\alpha_3 \pi S_1 R^2} + \frac{\pi R_{S_1} R^2}{\alpha_3 \pi S_1 R}} (2^{R_2} - 1),$$  \(32\)

respectively. We note that HD relaying is known to suffer from a spectral efficiency loss compared to FD relaying due to its time-orthogonal relay listening/forwarding suffering, so half duplex suffer from 50% loss in data rate, there is 1/2 factor in both data transmission and eavesdropping capacities [9].
B. Optimization of the Power Allocation Parameter \( \alpha_5 \) and Effect Secrecy Throughout

The optimal value of power allocation parameter \( \alpha_5 \) that minimizes the exact SOP given (27) can be obtained though

\[
\alpha_5^* = \arg \min_{0 \leq \alpha_5 < 1} P_{out}^{\text{NOMA-ANFDR}}.
\]

We first analytically determine the first-order derivative of \( P_{out}^{\text{NOMA-ANFDR}} \) with respect to \( \alpha_5 \) for a given \( \alpha_3 \) and \( \alpha_4 \). We numerically find that \( \frac{\partial P_{out}^{\text{NOMA-ANFDR}}}{\partial \alpha_5} \) is first negative and then positive. We then analytically determine the second-order derivative of \( P_{out}^{\text{NOMA-ANFDR}} \) with respect to \( \alpha_5 \) for given \( \alpha_3 \) and \( \alpha_4 \). We numerically find that \( \frac{\partial^2 P_{out}^{\text{NOMA-ANFDR}}}{\partial \alpha_5^2} \) is always positive when \( 0 < \alpha_5 < 1 \). Therefore, we conjecture that there is a unique value of \( \alpha_5 \) within \( 0 < \alpha_5 < 1 \), referred to as \( \alpha_5^* \), which achieves the minimum \( P_{out}^{\text{NOMA-ANFDR}} \). This conjecture will be supported by the numerical results in Section V. We denote \( P_{out}^{\text{NOMA-ANFDR}} \) as minimum exact SOP achieved by setting \( \alpha_5 = \alpha_5^* \) in (27).

In this paper, the EST is defined as the product of the secrecy rate and the maximum secure transmission probability (i.e., the minimum SOP), which is given by

\[
T_{\text{NOMA-AHRS}} = (R_1 + R_2)(1 - P_{out}^{\text{NOMA-AFQRS}}),
\]

where \((1 - P_{out}^{\text{NOMA-ANFDR}})\) means the transmission from the source was successfully received by the destination for both \( S_1 - D_1 \) and \( S_2 - D_2 \) user pairs, but not at eavesdroppers.

V. NUMERICAL RESULTS

In this section, we provide numerical results to examine the secrecy performance of the proposed NOMA-ANFDR scheme. The NOMA-ANHDR scheme and NOMA in cooperative half-duplex-relay without considering security (NOMA-HDR-w/o-SE, without considering the presence of eavesdroppers [5]) is also shown as benchmarks in the figures. We assume that all nodes are assumed to be collinear with \( d_{1R} = 0.2, d_{2R} = 0.5, d_{RD_1} = 0.8, d_{RD_2} = 0.6 \), and \( \nu = 4 \). We also assume that employing fixed transmit power allocation for legal users in these NOMA schemes. We set \( \alpha_1 = 0.9, \alpha_2 = 0.1, \alpha_3 = 9\alpha_4, R_1 = 0.5, R_2 = 1, P_S = P_R = 20\text{dB}, \) and \( P_E = 2\text{dB} \).

Fig. 2 plots the SOPs of the proposed NOMA-ANFDR scheme, NOMA-ANHDR scheme, and NOMA-HDR-w/o-SE with \( K = 3 \) and \( K = 6 \). We first see that the SOPs of the proposed NOMA-ANFDR and NOMA-ANHDR schemes first decrease and then increase as \( \alpha_5 \) increases, which implies that there is a unique \( \alpha_5 \) that minimizes the SOP, i.e., \( \alpha_5^* \). This supports our conjecture on \( \alpha_5 \) in Section IV. Secondly, it is observed from Fig. 2 that the theoretic SOPs achieved by the proposed NOMA-ANFDR and NOMA-ANHDR schemes match their simulated SOPs. This confirms the correctness of the results present in (27) and (28). Thirdly, it is observed from Fig. 2 that, both the SOPs of the proposed NOMA-ANFDR and NOMA-ANHDR schemes perform better than NOMA-HDR-w/o-SE. This indicates that artificial-noise enhances the physical layer security against eavesdropping attack. It is also observed from Fig. 2 that the NOMA-ANHDR scheme significantly outperforms the NOMA-ANHDR scheme, illustrating the security benefits of exploiting the FD mode to prevent eavesdropping attacks.

Fig. 3 plots minimum SOPs versus \( P_R \) with \( P_{RR} = 0\text{dB} \) and \( P_{RR} = 4\text{dB} \). We see that the minimum SOPs of the three schemes tend to decrease with \( P_R \), but the proposed NOMA-ANFDR scheme achieves a best performance, and the NOMA-HDR-w/o-SE scheme has the worst secrecy performance as compared to other AN-aided schemes, showing that the secur-
decreases, e.g., from NOMA-ANHDR scheme becomes more prominent as secrecy performance of the NOMA-ANFDR scheme relative defending against eavesdropping. It is also from Fig. 3 that the ty benefits of the exploiting AN-aided and FD mode in relay in
Fig. 3. Minimum secrecy outage probabilities versus $P_R$ with $K = 3$, $R_1 = 0.5$, $R_2 = 1$, $\pi_{RR} = 2$dB, $\pi_{RE} = 0$dB, and $\pi_{RR} = 4$dB.

ty benefits of the exploiting AN-aided and FD mode in relay in
defending against eavesdropping. It is also from Fig. 3 that the
secrecy performance of the NOMA-ANFDR scheme relative
to NOMA-ANHDR scheme becomes more prominent as $\pi_{RR}$ decreases, e.g., from $\pi_{RR} = 4$ dB to $\pi_{RR} = 0$ dB. This can be explained by the fact that the NOMA-ANFDR scheme has a better secrecy performance than the NOMA-ANHDR scheme when the self-interference is well suppressed.

Fig. 4 plots the EST versus $R_2$. One can observe that the
NOMA-ANFDR scheme achieves the highest EST since it has the
lowest minimum SOP among the three schemes. It is also from Fig. 4 that the proposed NOMA-ANFDR scheme can use a highest secure transmission rate for $S_2 - D_2$ user pair when the case of achieving the highest EST.

VI. CONCLUSIONS

In this paper, we proposed a new NOMA-ANFDR scheme in a cooperative relay network in the presence of $K$ eavesdroppers. To analyze the benefits of the NOMA-ANFDR scheme, we derive its SOP in closed form. It was shown that the NOMA-ANFDR scheme significantly outperforms the NOMA-ANHDR and the NOMA-HDR-w/o-SE scheme by achieving a lowest SOP and a highest EST. This result indicates that adopting the joint of FD and AN techniques at relays can greatly improve the physical layer security in cooperative NOMA systems.

ACKNOWLEDGEMENT

The authors would like to acknowledge that this work was partially supported by the National Natural Science Foundation of China (61671252, 61501251, 61571233, 61772287), the Key Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 14KJA510003, and the Australian Research Council Discovery Project (D-P150103905).

REFERENCES


