Secure Transmission Design for Cooperative NOMA in the Presence of Internal Eavesdropping

Binbin Su, Wenjuan Yu, Hongbo Liu, Arsenia Chorti, H. Vincent Poor

Secure Transmission Design for Cooperative NOMA in the Presence of Internal Eavesdropping

Binbin Su, Wenjuan Yu, *Member*, *IEEE*, Hongbo Liu, Arsenia Chorti, *Senior Member*, *IEEE* and H. Vincent Poor, *Life Fellow*, *IEEE*

***Abstract*—The application of successive interference cancellation (SIC) introduces critical security risks to cooperative non-orthogonal multiple access (NOMA) systems in the presence of untrustworthy network nodes, referred to as internal eavesdroppers. To address this potential security and reliability flaw, by assuming all users are untrusted, this letter investigates the effective secrecy throughput (EST) for a cooperative NOMA system, where a near user serves as an amplify-and-forward relay to help forward the information of a far user. Considering the inverse power allocation and SIC decoding order, a novel jamming strategy is proposed to enhance the security performance of the far user. Gauss-Chebyshev approximations of ESTs over Nakagami-m channels are derived. Asymptotic EST expressions are proposed to provide further insights. Numerical results demonstrate that the proposed jamming strategy and the inverse power allocation and SIC decoding order are both essential for achieving positive secrecy rates for both users.**

***Index Terms*-Non-orthogonal multiple access, untrusted internal users, effective secrecy throughput**

I. Introduction

Non-orthogonal multiple access (NOMA) has drawn significant attention due to its potential to improve spectral efficiency by serving multiple users over a single resource block [1]. Moreover, cooperative NOMA is regarded as an effective way to guarantee fairness among users, where a near NOMA user acts as a relay to help establish connections between the base station (BS) and far weak users [2]. However, due to the broadcast nature of wireless communication networks as well as the application of successive interference cancellation (SIC), NOMA is faced with severe security concerns [3], [4]. The security performance of cooperative NOMA with external eavesdropping has been studied in [5]–[7]. Furthermore, as network nodes of NOMA systems may be untrusted, NOMA systems are exposed to risks of internal eavesdropping. Secure transmission for non-cooperative NOMA systems with internal eavesdropping has been investigated in [8]–[10].

Note that the above studies either consider cooperative NOMA with external eavesdropping [5]–[7], or non-cooperative with only one untrusted user [8]–[10]. For cooperative NOMA systems, since SIC can be applied at all users [8], on one hand, it is difficult to achieve positive secrecy rates for a far user since an untrusted near user can easily intercept messages intended for the former due to the stronger channel gain between the BS and the near user [11]. On the other hand, an untrusted far user may access the information of a near user, which results in confidential information leakage. Therefore, for cooperative NOMA in the presence of internal eavesdropping, both near user and far user are faced with risks of being eavesdropped upon, and it is of importance to study security issues for cooperative NOMA with untrusted users.

We have, however, noticed that the effective secrecy throughput (EST), a measure of the rate at which information can be transferred securely in the presence of eavesdroppers [12], has not been studied for cooperative NOMA with untrusted internal adversaries. In this letter, we propose an approach to secure the transmissions in a two-user cooperative NOMA, using EST as the performance metric[1], for situations in which a near user U_1 plays the role of an amplify-and-forward (AF) relay for a far user U_2. Different from [8]–[10], we consider a purely antagonistic network in which both U_1 and U_2 are untrusted, and can act as passive eavesdroppers intercepting confidential messages intended for the other user. More importantly, we consider the inverse power allocation and SIC decoding order of standard NOMA, i.e., more transmit power is allocated to U_1, so that U_1 should first decode its own message. It is noted that though less power is allocated to U_2, the reliability is still guaranteed in our model as EST ensures that the achievable data rate is larger than or equal to the rate requirement. To enhance security performance, a novel jamming strategy is proposed, where the jamming signal is sent by U_2 to confuse U_1. Compared with external jamming [10], [13], the proposed strategy avoids communication overhead, and the jamming can be eliminated by U_2 before decoding its own information.

In this letter, we show that jamming and inverting power allocation and SIC decoding order are both essential to achieve positive ESTs for both NOMA users. If we allocate more power to U_2, according to the standard NOMA, its message x_2 will be decodable at U_1 and thus is unprotected. If jamming is used to induce secrecy for x_2 leaving U_1 unable to decode x_2, then U_1 will not be able to decode its own message x_1 either (because of the SIC order). To validate the performance of the proposed strategy, Gauss-Chebyshev approximations are derived for the ESTs. Numerical results demonstrate that our jamming strategy outperforms the benchmark scheme and ensures positive secrecy rates for both users.

Binbin Su and Hongbo Liu are with the National Key Laboratory of Science and Technology on Vessel Integrated Power System, Naval University of Engineering, Wuhan, 430033, China (email: subinbinbin_sdu@yahoo.com, myspace218@163.com).

Wenjuan Yu is with the School of Computing and Communications, Lancaster University, Lancaster LA1 4YW, U.K. (email: w.yu8@lancaster.ac.uk).

Arsenia Chorti is with ETIS, UMR 8051, CY University, ENSEA, CNRS, France (email: arsenia.chorti@ensea.fr). Arsenia Chorti has been supported by the eNiGMA and PHEBE projects of the CYU Initiative of Excellence and the CNRS IEA project PEGASUS.

H. Vincent Poor is with the Department of Electrical and Computer Engineering, Princeton University, Princeton NJ 08544 USA. (email: poor@princeton.edu).

[1]The considered two-user model can be easily extended to multiple NOMA clusters by performing user pairing, where each cluster is composed of a near user and a far user. By allocating orthogonal frequency bands to different NOMA clusters, each NOMA pair can be managed independently.

II. System Model

Consider a cooperative NOMA system, which is composed of one BS and two users, i.e., a near user U_1 and a far user U_2. The BS transmits information to U_2 with the help of U_1, since there is no direct link between the BS and U_2 due to shadow fading and severe blocking. U_1 and U_2 are considered to be untrusted by each other, i.e., both U_1 and U_2 can act as internal eavesdroppers. Each node is equipped with a single antenna and operates in half-duplex mode. The channel coefficients between the BS and U_1, and from U_1 to U_2 are denoted as h_1 and h_{12}, respectively. All channels are assumed to experience Nakagami-m fading with $E[|h_i|^2] = \Omega_i$ and fading parameters $m_i, i = \{1, 12\}$.

During the first slot, the BS transmits the superimposed signals of x_1 and x_2 to the near user. Following Wyner's work on secrecy capacity [14], [15], x_1 and x_2 are coded as the code-word rates $(R_{1,t}, R_{2,t})$ and secrecy rates $(R_{1,s}, R_{2,s})$, respectively. Meanwhile, the far user transmits a jamming signal. The received signal at U_1 can be modeled as

$$y_1 = h_1(\sqrt{a_1 P_s}x_1 + \sqrt{a_2 P_s}x_2) + \sqrt{P_I}x_0 + n_1, \quad (1)$$

where P_s is the transmit power at the BS, a_1 and a_2 are the power coefficients of U_1 and U_2 with $a_1 + a_2 = 1$ and $a_1 > a_2$, n_1 denotes additive white Gaussian noise (AWGN) at U_1 with variance σ^2, x_0 is the jamming signal and P_I denotes the received jamming power at U_1.

Since more power is allocated to x_1, based on the principle of SIC, U_1 first decodes x_1 by treating x_2 as interference, and then U_1 may eavesdrop upon the signal of U_2, i.e., U_1 decodes x_2 after subtracting the decoded x_1. Therefore, the received signal-to-interference-ratio (SINR) of x_1 and the eavesdropped SINR of x_2 at U_1 can be expressed as

$$\gamma_1 = \frac{a_1\rho_s|h_1|^2}{a_2\rho_s|h_1|^2 + \rho_I + 1}, \quad (2a)$$

$$\gamma_{1\to 2} = \frac{a_2\rho_s|h_1|^2}{\rho_I + 1}, \quad (2b)$$

where $\rho_s = \frac{P_s}{\sigma^2}$ and $\rho_I = \frac{P_I}{\sigma^2}$.

During the second transmission slot, U_1 amplifies and forwards its received signal to U_2 with an amplifying coefficient G. So, the received signal at U_2 can be expressed as

$$y_2 = h_{12}y_1 G + n_2. \quad (3)$$

Here, $G = \sqrt{\frac{P_R}{P_s|h_1|^2 + P_I + \sigma^2}}$, where P_R denotes the transmit power at U_1, and n_2 is AWGN at U_2 with variance σ^2.

As x_1 is allocated with more power, x_1 is decoded by treating the signal of x_2 as noise. Consequently, at U_2, the received SINR to intercept the message intended for U_1 can be expressed as

$$\gamma_{2\to 1} = \frac{a_1\rho_s\rho_R|h_1|^2|h_{12}|^2}{a_2\rho_s\rho_R|h_1|^2|h_{12}|^2 + \rho_s|h_1|^2 + \rho_R|h_{12}|^2 + \rho_I + 1}, \quad (4)$$

where $\rho_R = \frac{P_R}{\sigma^2}$.

After subtracting the information of U_1 from the received signals, the received SINR of U_2 is given by

$$\gamma_2 = \frac{a_2\rho_s\rho_R|h_1|^2|h_{12}|^2}{\rho_s|h_1|^2 + \rho_R|h_{12}|^2 + \rho_I + 1}. \quad (5)$$

III. Secrecy Performance Analysis

In this section, EST is adopted as the performance metric. EST is defined as the average transmitted secrecy rate from transmitter to receiver without being successfully eavesdropped upon, which characterizes the reliability and security of the system.

A. Exact Expressions

The ESTs of U_1 and U_2 are defined as

$$\eta_1 = R_{1,s}\Pr[\gamma_1 > \theta_{1,t}, \gamma_{2\to 1} < \theta_{1,s}], \quad (6a)$$

$$\eta_2 = R_{2,s}\Pr[\gamma_2 > \theta_{2,t}, \gamma_{1\to 2} < \theta_{2,s}]. \quad (6b)$$

where $\theta_{1,t} = 2^{2R_{1,t}} - 1, \theta_{2,t} = 2^{2R_{2,t}} - 1, \theta_{1,s} = 2^{2(R_{1,t} - R_{1,s})} - 1$, and $\theta_{2,s} = 2^{2(R_{2,t} - R_{2,s})} - 1$.

By substituting (2a) and (4) into (6a), we can derive that

$$\eta_1 = R_{1,s}\Pr\Big[(a_1 - a_2\theta_{1,t})\rho_s|h_1|^2 > (\rho_I + 1)\theta_{1,t}, \frac{a_1 - a_2\theta_{1,s}}{\theta_{1,s}} < \frac{\rho_s|h_1|^2 + \rho_R|h_{12}|^2 + \rho_I + 1}{\rho_s\rho_R|h_1|^2|h_{12}|^2}\Big]. \quad (7)$$

Clearly, when $a_1 - a_2\theta_{1,t} < 0$, $\eta_1 = 0$. Since $\theta_{1,t} \geq \theta_{1,s}$, on the condition that $a_1 - a_2\theta_{1,t} > 0$, (7) can be rewritten as

$$\eta_1 = R_{1,s}\Pr[\rho_s|h_1|^2 > \chi_1, \frac{\rho_s\rho_R|h_1|^2|h_{12}|^2}{\rho_s|h_1|^2 + \rho_R|h_{12}|^2 + \rho_I + 1} < \chi_2], \quad (8)$$

where $\chi_1 = \frac{(\rho_I + 1)\theta_{1,t}}{a_1 - a_2\theta_{1,t}}$, and $\chi_2 = \frac{\theta_{1,s}}{a_1 - a_2\theta_{1,s}}$.

To investigate the security of cooperative NOMA with jamming signals, the following theorem is presented to provide an approximation for η_1.

Theorem 1: An approximation of η_1 is given as (9), shown at the top of the next page, where P_1 is given in (10), $\lambda_{1,l} = \frac{\frac{(\rho_I+1)\theta_{1,t}}{a_1 - a_2\theta_{1,t}} + \frac{\theta_{1,s}}{a_1 - a_2\theta_{1,s}}}{2} + \frac{\frac{(\rho_I+1)\theta_{1,t}}{a_1 - a_2\theta_{1,t}} - \frac{\theta_{1,s}}{a_1 - a_2\theta_{1,s}}}{2}\delta_l$, $\delta_l = \cos(\frac{(2l-1)\pi}{2L})$, and $U(x) = \begin{cases} 1, & x > 0 \\ 0. & x \leq 0 \end{cases}$.

Proof: By denoting $X = \rho_s|h_1|^2$ and $Y = \rho_R|h_{12}|^2$ with $E[X] = \Omega_X$ and $E[Y] = \Omega_Y$, and fading parameters m_X and m_Y, the probability term in η_1 can be expressed as

$$\begin{aligned} P &= \Pr[X > \chi_1, \frac{XY}{X + Y + \rho_I + 1} < \chi_2] \\ &= \Pr[X > \chi_1, (X - \chi_2)Y < \chi_2(X + \rho_I + 1)]. \end{aligned} \quad (11)$$

Based on the values of χ_1 and χ_2, two cases are considered: Case 1: $\chi_1 \leq \chi_2$; Case 2: $\chi_1 > \chi_2$.

For Case 1, the above probability can be expressed as

$$P_1 = \int_{\chi_1}^{\chi_2} f_X(x)dx + \int_{\chi_2}^{\infty}\int_0^{\frac{\chi_2(x+\rho_I+1)}{x-\chi_2}} f_Y(y)f_X(x)dydx. \quad (12)$$

By inserting the cumulative distribution function (CDF) $F_X(x) = 1 - \sum_{r=0}^{m_X-1}(\frac{m_X x}{\Omega_X})^r \frac{1}{r!}e^{-\frac{m_X x}{\Omega_X}}$ and probability density function (PDF) $f_Y(y) = (\frac{m_Y}{\Omega_Y})^{m_Y}\frac{y^{m_Y-1}}{\Gamma(m_Y)}e^{-\frac{m_Y y}{\Omega_Y}}$, (12) can be rewritten as

$$P_1 = \sum_{r=0}^{m_X-1}(\frac{m_X\chi_1}{\Omega_X})^r\frac{1}{r!}e^{-\frac{m_X\chi_1}{\Omega_X}} - \sum_{r=0}^{m_Y-1}(\frac{m_X}{\Omega_X})^{m_X}\frac{1}{r!}\frac{1}{\Gamma(m_X)}$$

$$\eta_1 = U(a_1 - a_2\theta_{1,t})R_{1,s}\left(U(\chi_2-\chi_1)P_1 + U(\chi_1-\chi_2)(P_1 - \sum_{l=1}^{L}\sum_{r=0}^{m_{12}-1}(\frac{m_1}{\Omega_1})^{m_1}\frac{1}{r!}\frac{1}{\Gamma(m_1)}\omega_l\sqrt{(\lambda_{1,l}-\chi_2)(\chi_1-\lambda_{1,l})}\right.$$
$$\left.\times(\frac{m_{12}\chi_2(\lambda_{1,l}+\rho_I+1)}{\Omega_{12}(\lambda_{1,l}-\chi_2)})^r e^{-(\frac{m_{12}\chi_2(\lambda_{1,l}+\rho_I+1)}{\Omega_{12}(\lambda_{1,l}-\chi_2)}+\frac{m_1\lambda_{1,l}}{\Omega_1})}\lambda_{1,l}^{m_1-1}\right), \quad (9)$$

where $P_1 = \sum_{r=0}^{m_1-1}(\frac{m_1\chi_1}{\rho_s\Omega_1})^r\frac{1}{r!}e^{-\frac{m_1\chi_1}{\rho_s\Omega_1}} - \sum_{r=0}^{m_{12}-1}\sum_{s=0}^{r}\sum_{t=0}^{m_1-1}\binom{r}{s}\binom{m_1-1}{t}(\frac{m_1}{\rho_s\Omega_1})^{m_1}(\frac{m_{12}\chi_2}{\rho_R\Omega_{12}})^r e^{-\chi_2(\frac{m_1}{\rho_s\Omega_1}+\frac{m_{12}}{\rho_R\Omega_{12}})}$
$$\times\frac{1}{r!}(\chi_2+\rho_I+1)^s\chi_2^{m_1-1-t}\frac{2}{\Gamma(m_1)}K_{t-s+1}2\sqrt{\frac{m_1m_{12}\chi_2(\chi_2+\rho_I+1)}{\rho_s\rho_R\Omega_1\Omega_{12}}}\left(\frac{m_{12}\rho_s\Omega_1\chi_2(\chi_2+\rho_I+1)}{m_1\rho_R\Omega_{12}}\right)^{\frac{t-s+1}{2}}, \quad (10)$$

$$\eta_2 = U(\theta_{2,s}(\rho_I+1)-\theta_{2,t})R_{2,s}\sum_{l=1}^{L}\sum_{r=0}^{m_{12}-1}(\frac{m_1}{\rho_s\Omega_1})^{m_1}\frac{1}{\Gamma(m_1)}\frac{1}{r!}\omega_l\sqrt{(\lambda_{2,l}-\frac{\theta_{2,t}}{a_2})(\frac{\theta_{2,s}(\rho_I+1)}{a_2}-\lambda_{2,l})}(\frac{m_{12}\phi(\lambda_{2,l})}{\rho_R\Omega_{12}})^r\lambda_{2,l}^{m_1-1}$$
$$\times e^{-(\frac{m_1\lambda_{2,l}}{\rho_s\Omega_1}+\frac{m_{12}\phi(\lambda_{2,l})}{\rho_R\Omega_{12}})}, \quad (17)$$

$$\times\int_{\chi_2}^{\infty}(\frac{m_Y\chi_2(x+\rho_I+1)}{\Omega_Y(x-\chi_2)})^r e^{-\frac{m_Y\chi_2(x+\rho_I+1)}{\Omega_Y(x-\chi_2)}}x^{m_X-1}e^{-\frac{m_Xx}{\Omega_X}}dx$$
$$\overset{a}{=} P_1^1 - \sum_{r=0}^{m_Y-1}\sum_{s=0}^{r}\sum_{t=0}^{m_X-1}\binom{r}{s}\binom{m_X-1}{t}(\frac{m_X}{\Omega_X})^{m_X}\frac{1}{r!}(\frac{m_Y\chi_2}{\Omega_Y})^r$$
$$\times e^{-\chi_2(\frac{m_X}{\Omega_X}+\frac{m_Y}{\Omega_Y})}(\chi_2+\rho_I+1)^s\chi_2^{m_X-1-t}\frac{1}{\Gamma(m_X)}$$
$$\times\int_{\chi_2}^{\infty}(x-\chi_2)^{t-s}e^{-\left(\frac{m_X(x-\chi_2)}{\Omega_X}+\frac{m_Y\chi_2(\chi_2+\rho_I+1)}{\Omega_Y(x-\chi_2)}\right)}dx$$
$$\overset{b}{=} P_1^1 - \sum_{r=0}^{m_Y-1}\sum_{s=0}^{r}\sum_{t=0}^{m_X-1}\binom{r}{s}\binom{m_X-1}{t}(\frac{m_X}{\Omega_X})^{m_X}\frac{1}{r!}(\frac{m_Y\chi_2}{\Omega_Y})^r$$
$$\times e^{-\chi_2(\frac{m_X}{\Omega_X}+\frac{m_Y}{\Omega_Y})}(\chi_2+\rho_I+1)^s\chi_2^{m_X-1-t}\frac{2}{\Gamma(m_X)}$$
$$\times K_{t-s+1}\left(2\sqrt{\frac{m_Xm_Y\chi_2(\chi_2+\rho_I+1)}{\Omega_X\Omega_Y}}\right)$$
$$\times\left(\frac{m_Y\Omega_X\chi_2(\chi_2+\rho_I+1)}{m_X\Omega_Y}\right)^{\frac{t-s+1}{2}}, \quad (13)$$

where (a) is derived by denoting $P_1^1 \triangleq \sum_{r=0}^{m_X-1}(\frac{m_X\chi_1}{\Omega_X})^r\frac{1}{r!}e^{-\frac{m_X\chi_1}{\Omega_X}}$, (b) is obtained by adopting [16, Eq. (3.478,4)], and $K_v(z)$ represents the Bessel functions of imaginary argument [17].

For Case 2, the probability in (11) can be reformulated as

$$P_2 = \int_{\chi_1}^{\infty}\int_{0}^{\frac{\chi_2(x+\rho_I+1)}{x-\chi_2}} f_Y(y)f_X(x)dydx$$
$$= P_1 + \int_{\chi_2}^{x_1}\int_{0}^{\frac{\chi_2(x+\rho_I+1)}{x-\chi_2}} f_Y(y)f_X(x)dydx. \quad (14)$$

By applying Gauss-Chebyshev integration, the approximation for P_2 can be given by

$$P_2 = P_1 + \sum_{l=1}^{L}\sum_{r=0}^{m_Y-1}(\frac{m_X}{\Omega_X})^{m_X}\frac{1}{r!}\frac{1}{\Gamma(m_X)}\omega_l\lambda(l)^{m_X-1}$$
$$\times\sqrt{(\lambda_l-\chi_2)(\chi_1-\lambda_l)}(\frac{m_Y\chi_2(y(l)+\rho_I+1)}{\Omega_Y(y(l)-\chi_2)})^r$$
$$\times e^{-(\frac{m_Y\chi_2(y(l)+\rho_I+1)}{\Omega_Y(y(l)-\chi_2)}+\frac{m_Xy(l)}{\Omega_X})}, \quad (15)$$

where $\omega_l = \frac{\pi}{L}$, L denotes the approximation order for Gauss-Chebyshev integration, $\lambda_l = \frac{\chi_1+\chi_2}{2} + \frac{\chi_1-\chi_2}{2}\delta_l$, and $\delta_l = \cos(\frac{(2l-1)\pi}{2L})$.

Hence, a complete analytical expression for the probability term in η_1 can be written as $P = U(\chi_2-\chi_1)P_1 + U(\chi_1-\chi_2)P_2$. Then, (9) can be derived via replacing Ω_X and Ω_Y with $\rho_s\Omega_1$ and $\rho_R\Omega_{12}$, respectively.

Remark 1: According to (9), η_1 is a monotonically decreasing function of P_R and P_I, but increases monotonically with P_s. Moreover, the power allocation factors and the code-word rate need to be carefully set to satisfy $a_1 - a_{2\theta_{1,t}} > 0$ to achieve nonzero η_1.

For η_2, by substituting (2b) and (5) into (6b), we have

$$\eta_2 = R_{2,s}\Pr[\frac{\rho_s\rho_R|h_1|^2|h_{12}|^2}{\rho_s|h_1|^2+\rho_R|h_{12}|^2+\rho_I+1} > z_1, \rho_s|h_1|^2 < z_2], \quad (16)$$

where $z_1 = \frac{\theta_{2,t}}{a_2}$ and $z_2 = \frac{\theta_{2,s}(\rho_I+1)}{a_2}$.

Theorem 2: An exact expression for η_2 is given in (17), shown at the top of this page, where $\lambda_{2,l} = \frac{\frac{\theta_{2,t}}{a_2}+\frac{\theta_{2,s}(\rho_I+1)}{a_2}}{2} + \frac{\frac{\theta_{2,t}}{a_2}-\frac{\theta_{2,s}(\rho_I+1)}{a_2}}{2}\delta_l$, $\delta_l = \cos(\frac{(2l-1)\pi}{2L})$, and $\phi(x) = \frac{\theta_{2,t}(x+\rho_I+1)}{a_2x-\theta_{2,t}}$.

Proof: By denoting $X = \rho_s|h_1|^2$ and $Y = \rho_R|h_{12}|^2$, the probability term in η_2 can be written as

$$P = \Pr[X < z_2, \frac{XY}{X+Y+\rho_I+1} > z_1]$$
$$= \sum_{r=0}^{m_Y-1}(\frac{m_X}{\Omega_X})^{m_X}\frac{1}{\Gamma(m_X)}\frac{1}{r!}\int_{z_1}^{z_2}(\frac{m_Y\phi(x)}{\Omega_Y})^r x^{m_X-1}$$
$$\times e^{-(\frac{m_Xx}{\Omega_X}+\frac{m_Y\phi(x)}{\Omega_Y})}dx, \quad (18)$$

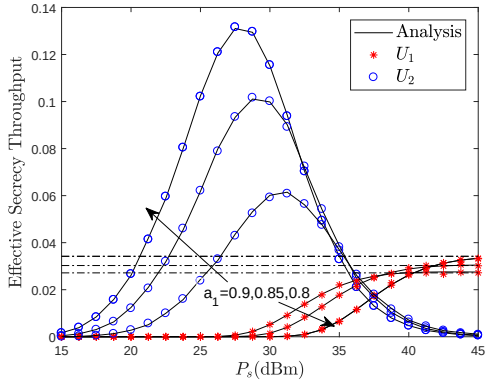


Fig. 1. The ESTs of U_1 and U_2 vs. P_s with $P_R = -2$ dBm and $P_I = -10$ dBm.

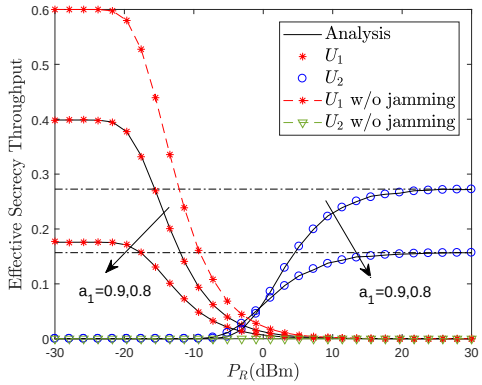


Fig. 2. The ESTs of U_1 and U_2 vs. P_R with $P_s = 36$ dBm and $P_I = -10$ dBm.

where $\phi(x) = \frac{z_1(x+\rho_I+1)}{x-z_1}$.

By employing Gauss-Chebyshev integration, the approximation for (18) is derived as

$$P = \sum_{l=1}^{L}\sum_{r=0}^{m_Y-1}(\frac{m_X}{\Omega_X})^{m_X}\frac{1}{\Gamma(m_X)}\frac{1}{r!}\omega_l\sqrt{(\lambda_l-z_1)(z_2-\lambda_l)} \times\left(\frac{m_Y\phi(\lambda_l)}{\Omega_Y}\right)^r y_l^{m_X-1}e^{-(\frac{m_X y_l}{\Omega_X}+\frac{m_Y\phi(y_l)}{\Omega_Y})}, \quad (19)$$

where $\lambda_l = \frac{z_1+z_2}{2} + \frac{z_1-z_2}{2}\delta_l$, and $\delta_l = \cos(\frac{(2l-1)\pi}{2L})$.

By replacing Ω_X and Ω_Y with $\rho_s\Omega_1$ and $\rho_R\Omega_{12}$, and after some algebraic manipulations, an approximation for η_2 can be finally given in (17).

Remark 2: (17) indicates that η_2 is not a monotonic function of either P_s or P_I, thus P_s and P_I should be carefully chosen. Particularly, a nonzero η_2 can only be obtained under the condition that $\rho_I > \frac{\theta_{2,t}}{\theta_{2,s}} - 1$, which shows that jamming is essential for the secure transmission of U_2. Note that an infinite P_I results in zero η_2, which reveals that η_2 can be maximized with an optimal P_I.

B. Asymptotic Expressions

Based on the derived expressions for η_1 and η_2, we can see that the infinite P_R and P_I result in zero η_1, and η_2 becomes zero with infinite P_s. Thus, we provide an asymptotic expression for η_1 as $P_s \to \infty$, and one for η_2 as $P_R \to \infty$.

When $P_s \to \infty$ and $a_1 - a_2\theta_{1,t} > 0$, η_1 can be expressed as

$$\eta_1^{P_s\to\infty} = R_{1,s}[\rho_R|h_{12}|^2 < \frac{\theta_{1,s}}{a_1 - a_2\theta_{1,s}}]. \quad (20)$$

By employing the CDF $F_X(x) = 1 - \sum_{r=0}^{m_X-1}(\frac{m_X x}{\Omega_X})^r\frac{1}{r!}e^{-\frac{m_X x}{\Omega_X}}$, we can derive an asymptotic closed-form expression for η_1 as

$$\eta_1^{P_s\to\infty} = R_{1,s}\left(1 - \sum_{r=0}^{m_{12}-1}(\frac{m_{12}\theta_{1,s}}{(a_1-a_2\theta_{1,s})\rho_R\Omega_{12}})^r\frac{1}{r!} \times e^{-\frac{m_{12}\theta_{1,s}}{(a_1-a_2\theta_{1,s})\rho_R\Omega_{12}}}\right). \quad (21)$$

When $P_R \to \infty$, an asymptotic closed-form expression for η_2 can be written as

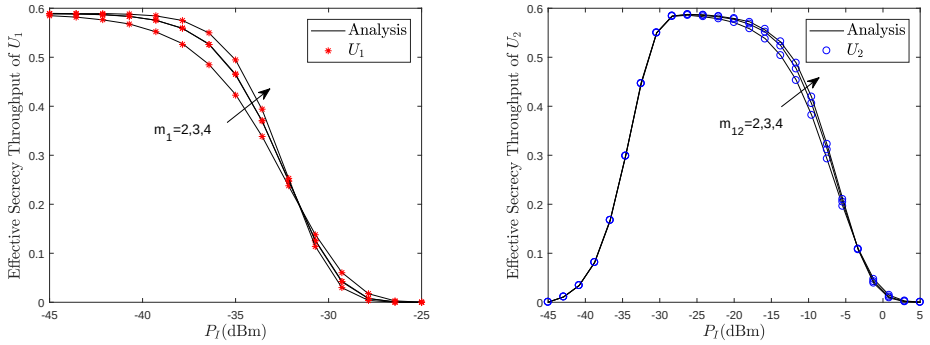
$$\eta_2^{P_R\to\infty} = R_{2,s}\left(\sum_{r=0}^{m_1-1}(\frac{m_1\theta_{2,t}}{a_2\rho_s\Omega_1})^r\frac{1}{r!}e^{-\frac{m_1\theta_{2,t}}{a_2\rho_s\Omega_1}} - \sum_{r=0}^{m_1-1}(\frac{m_1\theta_{2,s}(\rho_I+1)}{a_2\rho_s\Omega_1})^r\frac{1}{r!}e^{-\frac{m_1\theta_{2,s}(\rho_I+1)}{a_2\rho_s\Omega_1}}\right). \quad (22)$$

Remark 3: According to (21) and (22), we can see that the ESTs of U_1 and U_2 tend to nonzero constants when $P_s \to \infty$ and $P_R \to \infty$, respectively, as $\eta_1^{P_s\to\infty}$ is determined by the second slot, while $\eta_2^{P_R\to\infty}$ is determined by the first slot.

IV. Numerical Results

In this section, we present numerical results to evaluate the performance of the proposed cooperative NOMA system. The parameters are set as follows, unless otherwise stated. The average channel gains are chosen as $\Omega_i = \frac{1}{d_i^\alpha}$, where $i \in \{1, 12\}$, the distance $d_i = 20m$, and $\alpha = 2.7$ denoting the path loss exponent. Without loss of generality, we set $L = 50$, $R_{1,t} = R_{2,t} = 1$ BPCU, $R_{1,s} = R_{2,s} = 0.6$ BPCU, and uniform Nakagami-m fading is assumed for all channels, where $m_1 = m_{12} = 2$. The background noise power is assumed to be -50 dBm.

In Fig. 1, the relationship between the EST and the transmit power at the BS (P_s) is presented. As can be observed from Fig. 1, the derived analytical results are consistent with those from the simulations, and both users can achieve positive secrecy rate when P_s ranges from 33 dBm to 42 dBm. We can see that increasing P_s enhances the secrecy performance of U_1, and the EST of U_1 converges to asymptotic values as P_s gradually increases. Moreover, the EST of U_2 first increases and then decreases, which reveals that there exists an optimal P_s to maximize the EST of U_2. In addition, for the near user U_1, decreasing the power allocation fraction at the near user results in better secrecy performance in the low transmit power regime, while better system performance can be achieved when a larger power is allocated to the near user in the high transmit power region. However, the relationship between the far user U_2 and the power coefficient a_1 is inverse to that of U_1 and a_1. The reason for this is that, the impact of the jamming signal is negligible when P_s becomes larger.



(a) The EST of U_1 vs. P_I with $P_s = 10$ dBm and $P_R = -20$ dBm

(b) The EST of U_2 vs. P_I with $P_s = 10$ dBm and $P_R = 20$ dBm

Fig. 3. The ESTs vs. P_I.

Fig. 2 plots the ESTs of U_1 and U_2 versus P_R with $P_s = 36$ dBm and $P_I = -10$ dBm. Cooperative NOMA without jamming, namely 'U_1 w/o jamming' and 'U_2 w/o jamming', is plotted as the comparison scheme. For cooperative NOMA without jamming, we can see that though the EST of U_1 outperforms that of the proposed jamming strategy, the EST of U_2 remains at zero, thus indicating that U_2 cannot achieve secure transmission. The derived analytical results coincide precisely with those of the simulations. We can see that the EST of U_1 decreases with P_R, and the EST of U_2 converges to asymptotic values as P_R increases. This is because increasing P_R results in a larger achievable rate of U_2 as well as a larger interception rate for U_2 detecting the information of U_1. Moreover, U_1 can always benefit from the larger power allocated to the near user, while increasing a_1 degrades the secrecy performance of U_2 in the low P_R region, but improves the EST of U_2 when P_R becomes larger. The reason for this is that, for the data rate of U_2, the impact of the power allocation factor a_2 overwhelms the effect of P_R when P_R is relatively small, and P_R plays the leading role in the high power region.

In Fig. 3, the ESTs of U_1 and U_2 versus P_I are presented, respectively. As can be seen from Fig. 3. (a), the EST of U_1 decreases with P_I since P_I interferes the achievable SINR of U_1 as well as the intercept SINR of U_2. The EST of U_2 first increases and then decreases, thus an optimal P_I exists to maximize the EST. Moreover, for U_1 and U_2, more stable channels, i.e., larger Nakagami-m fading parameters, contribute to the improvement of the EST in the low power regime, and degrade the secrecy performance with a higher P_I.

V. Conclusion

In this letter, to address open security issues for a two-user cooperative NOMA network, the inverse power allocation and SIC decoding order as well as a novel jamming strategy have been proposed to overcome information leakage in the presence of internal untrusted near and far users. To evaluate the performance of the proposed system, Gauss-Chebyshev approximations and an asymptotic analysis of the ESTs have been derived for both users. Numerical results have validated that the proposed jamming strategy supports secure transmissions, while the jamming power needs to be chosen carefully to achieve satisfactory secrecy performance. The impacts of P_s and P_R on EST values have also been illustrated.

References

[1] Z. Ding, Z. Yang, P. Fan, and H. V. Poor. On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users. *IEEE Signal. Proc. Lett.*, vol. 21, no. 12, pp. 1501-1505, July 2014.

[2] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor. Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer. *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 938-953, Apr. 2016.

[3] L. Lv, H. Jiang, Z. Ding, Q. Ye, N. Al-Dhahir, and J. Chen. Secure non-orthogonal multiple access: An interference engineering perspective. *IEEE Network*, 2020, early access.

[4] W. Yu, A. Chorti, L. Musavian, H. V. Poor, and Q. Ni. Effective secrecy rate for a downlink NOMA network. *IEEE Trans. Wireless Commun.*, vol. 18, no. 12, pp. 5673-5690, Dec. 2019.

[5] R. Ruby, T. Riihonen, K. Wu, Y. Liu, and B. M. ElHalawany. Performance analysis of multi-phase cooperative NOMA systems under passive eavesdropping. *Signal Processing*, 182:107934, 2021.

[6] J. Chen, L. Yang, and M.-S Alouini. Physical layer security for cooperative NOMA systems. *IEEE Trans. Veh. Technol.*, 67(5):4645–4649, May 2018.

[7] B. M. ElHalawany, R. Ruby, T. Riihonen, and K. Wu. Performance of cooperative NOMA systems under passive eavesdropping. In *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pages 1–6. IEEE, Abu Dhabi, United Arab Emirates, Dec. 2018.

[8] B. M. ElHalawany and K. Wu. Physical-layer security of NOMA systems under untrusted users. In *Proc. IEEE GLOBECOM*, United Arab Emirates, pp. 1-6, Dec. 2018.

[9] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong. Secure transmission designs for NOMA systems against internal and external eavesdropping. *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930-2953, Mar. 2020.

[10] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong. Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper. *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13005-13017, Nov. 2020.

[11] S. Thapar, D. Mishra, and R. Saini. Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users. *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13259-13272, Sep. 2020.

[12] Z. Xiang, W. Yang, G. Pan, Y. Cai, and X. Sun. Secure transmission in non-orthogonal multiple access networks with an untrusted relay. *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 905-908, June 2019.

[13] C. Yu, HL. Ko, X. Peng, X. Xie, and P. Zhu. Jammer-aided secure communications for cooperative NOMA systems. *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 1935-1939, Nov. 2019.

[14] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[15] A. Chorti, C. Hollanti, JC. Belfiore, and H. V. Poor. *Physical layer security: A paradigm shift in data confidentiality*. Lecture Notes in Electrical Engineering. Springer Verlag, Germany, 2016.

[16] I. S. Gradshteyn and I. M. Ryzhik. *Table of Integrals*, series and products. 7th ed. New York, NY, USA: Academic, 2007.

[17] G. Dattoli and A. Torre. Theory and applications of generalized Bessel functions. Rome, Italy: Aracne Editrice, 1996.