# RESEARCH

# EURASIP Journal on Wireless Communications and Networking

# **Open Access**

# On the performance of physical layer security in virtual full-duplex non-orthogonal multiple access system



Weidong Guo<sup>1,2\*</sup> and Yuxi Liu<sup>3</sup>

\*Correspondence: gud2001@qfnu.edu.cn <sup>1</sup> School of Information Science and Engineering, Shandong University, 72 Binhai Road, Jimo 266237, Qingdao, P. R. China Full list of author information is available at the end of the article

# Abstract

This paper investigates physical layer security analysis of cooperative non-orthogonal multiple access (NOMA) communication system. A virtual full-duplex (VFD) relaying scheme with an untrusted amplify-and-forward (AF) half-duplex (HD) relay and a trusted decode-and-forward (DF) HD relay is used in this system to improve the spectral efficiency. In order to prevent the untrusted relay from eavesdropping, a simple and practical cooperative jamming scheme is designed to confuse the untrusted relay. The exact expressions of effective secrecy throughput (EST) for NOMA users and approximate expression of EST for non-NOMA user are derived. All theoretical results are validated by numerical simulations which demonstrate that the proposed VFD-NOMA scheme is superior to existing HD-NOMA scheme in cooperative system and jamming plays an important role for obtaining acceptable EST. In addition, simulation results shows that the best secrecy performance highly depends on the system parameters such as transmit powers and jamming signal power.

**Keywords:** Virtual full-duplex (VFD), Physical layer security, Non-orthogonal multiple access (NOMA), Effective secrecy throughput (EST)

# **1** Introduction

As one of the promising key techniques of the fifth-generation (5G) wireless networks, non-orthogonal multiple access (NOMA) has been applied in various areas [1, 2]. NOMA utilizes the power domain to achieve multiple access strategies, which is unlike the conventional orthogonal multiple access (OMA) structures. Since the NOMA technique exploits the new dimension of the power domain, it has the potential to be integrated with existing MA paradigms. On the other hand, the technique of cooperative transmission can form a virtual multiple-input multiple-output (MIMO) scheme to process data cooperatively, which can enhance the communication reliability for the users who are in poor channel conditions. It is reasonable to integrate NOMA into relaying networks. The authors in [3] proposed a new cooperative NOMA scheme and analyzed the outage probability and diversity gain of the system.

In the above references, all the relays are in half-duplex (HD) mode which requires additional bandwidth or time slot and reduces spectral efficiency of the system because



© The Author(s), 2021. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http:// creativecommons.org/licenses/by/4.0/.

the relay isolates the transmit and receive signals in two orthogonal time slots or frequency channels. To avoid this issue, full-duplex (FD) is proposed as a promising technique for the next generation wireless systems, because it can double the spectrum efficiency by realizing transmission and reception on the same carrier frequency, simultaneously [4]. Two main types of FD relay techniques, namely FD amplify-and-forward (AF) relaying and FD decode-and-forward (DF) relaying, have been discussed in [5, 6]. The authors in [7] propose an energy-efficient oriented algorithm for FD cooperative NOMA systems and demonstrate both significant energy-efficient and throughput enhancements over the HD cooperative NOMA and the prefixed FD cooperative NOMA regime. However, the significant amount of self-interference (SI) between transmitting and receiving radio frequency chains means that the performance of FD relay is degraded by the residual SI [8]. In [9], the authors provide a characterization of the distribution of the self-interference before and after active cancellation mechanisms. In [10], the author analyzed the outage probability, ergodic rate and energy efficiency of FD user relaying with imperfect SI cancellation.

Alternatively, we may instead consider a distributed version of a FD system, called virtual FD (VFD), where a pair of HD relays receive and transmit signals successively to imitate the operation of FD relay. This idea inherits the benefits of the FD system, while each relay requires only a single antenna, and the physical separation between the two HD relays eliminates the SI problem perfectly [8]. The combination of NOMA and VFD will further improve the spectrum efficiency. In [11], the authors found that VFD-NOMA system achieves a lower outage probability and a higher ergodic rate than the existing successive relaying OMA system and ideal FD-NOMA system. However, secrecy transmission of VFD cooperative NOMA system still remains unexplored.

In future networks, the ubiquitous connectivity makes our privacy and secrecy expose to radio space. Security becomes a major concern when designing communication systems. Due to the broadcast nature of radio propagation, wireless communication is vulnerable to be eavesdropped [12]. In relay-assisted NOMA networks, when the relay is untrusted, it may exploit these weaknesses to its benefit and behave as a passive eavesdropper who tries to listen in on an ongoing transmission [13]. Cooperative jamming has been become a promising technique to protect the transmission in untrusted relay OMA networks [14]. Authors in [15] describe the evolution of cooperative jamming transmission strategies from point-to-point channels to multiple antenna systems, followed by generalizations to larger multiuser networks. Choi and Lee [16] proposed a new cooperative jamming technique for an AF relay network with multiple relays, and the simulation results showed that the network with the proposed technique provides lower secrecy outage probability than a conventional scheme. The internal jamming strategy is employed in [17], where the legitimate user is enlisted as a jammer to distract the untrusted relay and adopts SI cancellation to eliminate the jamming. Yuan et al. [18] analyzed cooperative NOMA scheme, where the source actively sends jamming signals, while the relay is forwarding, thereby enhancing the security of intended communication links. In [19], a two-stage FD jamming scheme is proposed to ensure the secure transmission of cooperative NOMA users. Although beamforming of relay was designed in this paper to cancel the SI, when the estimation error of the channel state information (CSI) cannot be ignored, or the number of antennas at the relay is not enough to perform the beamforming, the residual self-interference channel still has to be considered. In this case, VFD-NOMA system is more practical because physical separation of relays eliminates the SI problem perfectly. But until now, there are few studies on the security performance of VFD-NOMA system.

According to the above references, this paper studies the cooperative VFD-NOMA transmission and investigated its secrecy performance with the presentence of an untrusted relay. The VFD system consists an untrusted AF relay and a trusted DF relay. Two users are served by the trusted relay using cooperative NOMA, and only one user is served by the untrusted relay because the untrusted relay is an eavesdropper. We assume that the untrusted relay can obtain messages of all users. A new cooperative jamming strategy is adopted to secure the transmission of untrusted relay link. The jamming signal transmitted by only one user is utilized to confuse the untrusted relay. The exact effective secrecy throughput (EST) expressions for NOMA users and approximate EST expression for non-NOMA user are derived, which shows that the jamming is indispensable for achieving nonzero EST. Our principal motivations and contributions are summarized as follows.

- As mentioned above, the combination of NOMA and VFD can improve the frequency efficiency and eliminate the residual SI of FD relaying simultaneously, but when we use VFD in a NOMA system, a pair of relays must be employed to form a VFD system and one of the relays may be an eavesdropper. There is still a paucity of research contributions on investigating the security issues of NOMA in a VFD system, which is the motivation of this paper. In order to improve the spectral efficiency, eliminate the residual SI of FD relaying and prevent untrusted relay eavesdropping simultaneously, we integrate NOMA, VFD and untrusted relay together and introduce a VFD relaying NOMA scheme in this study. The application scenario of this study is that multiple relays with one antenna can be employed to forward information, but some relays have poor credibility and could be eavesdroppers. We assume that in VFD relay system, one relay is trusted and the other is untrusted. To guarantee the secure transmission, a new cooperative jamming strategy is adopted to distract the untrusted relay. It is differing from [20] where jamming is transmitted by both the two users and our scheme saves the jamming power.
- The novelty of this study is that a novel cooperative jamming strategy is adopted to secure the untrusted relay VFD-NOMA networks and the EST expressions are derived to obtain further insights into parameters on system performance, which shows that there exist the optimal values of source power, relay power and jamming power. These findings are of great theoretical value for practical secure communication.

The rest of this paper is organized as follows. In Sect. 2, we introduce the system model. The closed-form expressions of EST are derived in Sect. 3. Numerical and simulations results are presented in Sect. 4, and conclusions are drawn in Sect. 5.

## 2 System model

As shown in Fig. 1, we consider a cooperative VFD-NOMA system, which consists of a source (S), a trusted DF relay (R), an untrusted AF relay (E) and three users (m, n, p). m is close to *n*, but they are far away from *p*. We assume that there do not exist direct links between S and users. R and E are willing to help the transmission. R can forward the information for m and n using NOMA, but it cannot forward information for p because they are too far apart. *E* is closer to *p* than *R* and can forward the information for *p*. But E is untrusted and can be regarded as potential Eves, so there is risk of leaking information of all users to E. All nodes are configured with one antenna and operate in HD mode. The channels between any transmitter and receiver are assumed to experience independent block Rayleigh fading, and the additive white Gaussian noise of all links has a zero mean and equal variance  $N_0$ . The channel coefficients between nodes are known as follows:  $h_{SR}$  denotes channel coefficient between S and R,  $h_{SE}$  denotes channel coefficient between S and E,  $h_{RE}$  denotes channel coefficient between R and E,  $h_{Sm}$  denotes channel coefficient between R and m,  $h_{Sn}$  denotes channel coefficient between R and n,  $h_{Ep}$  and denotes channel coefficient between E and p. The channel power gains of those hops  $|h_{SR}|^2$ ,  $|h_{SE}|^2$ ,  $|h_{RE}|^2$ ,  $|h_{Rm}|^2$ ,  $|h_{Rm}|^2$  and  $|h_{Ep}|^2$  are assumed to be exponentially distribution, and the corresponding instantaneous signal-to-noise ratios (SNRs)  $P_S |h_{SR}|^2 / N_0$ ,  $P_{S}|h_{SE}|^{2}/N_{0}, P_{R}|h_{RE}|^{2}/N_{0}, P_{R}|h_{Rm}|^{2}/N_{0}, P_{R}|h_{Rm}|^{2}/N_{0} \text{ and } P_{E}|h_{Ep}|^{2}/N_{0} \text{ are also expo$ nential random variables with parameters  $\lambda_1$ ,  $\lambda_2$ ,  $\lambda_3$ ,  $\lambda_4$ ,  $\lambda_5$  and  $\lambda_6$ ,, respectively.  $P_S$ ,  $P_R$ and  $P_E$  are the transmission power at *S*, *R* and *E*, respectively. We also assume that without loss of generality, channel gains are sorted as  $|h_{Rm}|^2 < |h_{Rn}|^2$ . The protocol of the VFD-NOMA scheme is divided into three equal time slots which is stated as follows.

During the first time slot, S broadcasts a superimposed mixture

$$x_s = \sqrt{a_m P_S x_m} + \sqrt{a_n P_S x_n},\tag{1}$$

where  $x_m$  and  $x_n$  are the signals for m and n, respectively, and  $E(x_m^2) = E(x_n^2) = 1$ . (E(·) denotes the expectation of a random variable.) Based on well-known Wyner secrecy code theorem [21],  $x_m$  and  $x_n$  are coded as  $(\tau_{m,t}, \tau_{m,s})$  and  $(\tau_{n,t}, \tau_{n,s})$ , respectively, where  $\tau_{m,t}$  and  $\tau_{n,t}$  are the codeword rates, and  $\tau_{m,s}$  and  $\tau_{n,s}$  are secrecy rates.  $a_m$  and  $a_n$  are the power split factors of signals  $x_m$  and  $x_n$ , respectively. Note that  $a_m + a_n = 1$  and  $a_m > a_n$  according to the principle of NOMA. In order to reduce the risk of leaking the information of m and n to E, at the same time, p is chosen to transmit a jamming signal to confuse E which is shown in the first part of Fig. 1. The observations at R and E are given by



$$y_R = h_{SR} \left( \sqrt{a_m P_S} x_m + \sqrt{a_n P_S} x_n \right) + n_R, \tag{2}$$

$$y_{E,1} = h_{SE} \left( \sqrt{a_m P_S} x_m + \sqrt{a_m P_S} x_n \right) + \sqrt{P_I} x_0 + n_E, \tag{3}$$

where  $n_R$  and  $n_E$  are the additive white Gaussian noises,  $x_0$  is the jamming signal, and  $P_I$  is the power of the received jamming at E. (The setting of  $P_I$  in our model is the same as [22]. We can also set an jamming transmission power at p and then consider the impacts of jamming power and jamming channel fading on the performance, but it will increase analysis complexity and we will discuss this setting in the future. In the numerical results part of this paper, we will investigate the impact of different values of  $P_I$  on the system performance.) As p and R are too far apart, there is no jamming signal in (2).

*R* is assumed to have the ability to apply successive interference cancellation (SIC). According to the principle of SIC,  $x_m$  is demodulated with the interference of  $x_m$  because  $x_m$  is allocated more power, and when  $x_m$  is demodulated successfully,  $x_n$  can be directly demodulated after subtracting the interference of  $x_m$  [23]. The received signal-to-interference-and-noise ratio (SINR) for decoding  $x_m$  at *R* can be written as

$$\gamma_{R \to m} = \frac{a_m |h_{SR}|^2 P_S}{a_n |h_{SR}|^2 P_S + N_0}.$$
(4)

After *R* successfully demodulates the signal of *m*, the interference from *m* can be eliminated by SIC. The SINR for decoding  $x_n$  at *R* can be written as

$$\gamma_{R \to n} = \frac{a_n P_S \left| h_{SR} \right|^2}{N_0}.$$
(5)

We consider the worst case that *E* has the ability to apply SIC and can always eliminate the interference from  $x_m$  while demodulating  $x_n$ . The SINRs of *E* wiretapping the message of *m* and *n* in first time slot can be written as

$$\gamma_{E \to m,1} = \frac{a_m P_S |h_{SE}|^2}{a_n P_S |h_{SE}|^2 + P_I + N_0},$$
(6)

$$\gamma_{E \to n,1} = \frac{a_n P_S |h_{SE}|^2}{P_I + N_0}.$$
(7)

During the second time slot, R re-encodes  $x_m$  and  $x_n$  and forwards it to m and n. The observations at m and n are given by

$$y_m = h_{Rm} \left( \sqrt{a_m P_R} x_m + \sqrt{a_n P_R} x_n \right) + n_0, \tag{8}$$

$$y_n = h_{Rn} \left( \sqrt{a_m P_R} x_m + \sqrt{a_n P_R} x_n \right) + n_0.$$
<sup>(9)</sup>

When *m* and *n* demodulate the message of *m*, the SINRs can be expressed as

$$\gamma_{m \to m} = \frac{a_m |h_{Rm}|^2 P_R}{a_n |h_{Rm}|^2 P_R + N_0},$$
(10)

$$\gamma_{n \to m} = \frac{a_m |h_{Rn}|^2 P_R}{a_n |h_{Rn}|^2 P_R + N_0}.$$
(11)

After n successfully demodulates the signal of m, the received SINR at n to decode its own signal is

$$\gamma_{n \to n} = \frac{a_n P_R \left| h_{Rn} \right|^2}{N_0}.$$
(12)

When *R* forwards the messages to *m* and *n* in this time slot, *S* transmits a new signal  $x_p$  of *p* to *E* with transmission power of  $P_S$  at the same time. Based on Wyner secrecy code theorem,  $x_p$  is coded as  $(\tau_{p,t}, \tau_{p,s})$ , where  $\tau_{p,t}$  is the codeword rate and  $\tau_{p,s}$  is secrecy rate. *E* can also receive the signal from *R* at this phase which is shown in the second part of Fig. 1. Similar to the first time slot, *p* also transmits the jamming signal  $x_0$  to *E* at this time slot. The observation at *E* is given by

$$y_{E,2} = h_{SE}\sqrt{P_S}x_p + h_{RE}\left(\sqrt{a_m P_R}x_m + \sqrt{a_m P_R}x_n\right) + \sqrt{P_I}x_0 + n_0.$$
 (13)

With this SINR, *E* can wiretap the message of *m*, *n* and *p*.  $x_p$  is decoded first because it has the most power, then  $x_m$  is decoded, and  $x_n$  is decoded at the end. The SINRs of *E* wiretapping the messages in this time slot can be written as

$$\gamma_{E \to p} = \frac{P_S |h_{SE}|^2}{P_R |h_{RE}|^2 + P_I + N_0},$$
(14)

$$\gamma_{E \to m,2} = \frac{a_m P_R |h_{RE}|^2}{a_n P_R |h_{RE}|^2 + P_I + N_0},$$
(15)

$$\gamma_{E \to n,2} = \frac{a_n P_R |h_{RE}|^2}{P_I + N_0}.$$
(16)

We assume that  $x_0$  is known by m and n and the corresponding term related to the jamming signal can be eliminated in (8) and (9). (This is a common assumption in the jamming literature [24–27] where the pre-defined jamming signal can be generated by using some pseudorandom codes that are known to m and n but not available to the curious untrusted relay. Transmission of the jamming signal from p to m and n can be accomplished by implementing the destination-based cooperative jamming technique.)

During the third time slot, *E* relays  $y_{E,2}$  to *p* using AF protocol with amplifying coefficient  $G = \sqrt{P_E / \left(P_S \left|h_{SE}\right|^2 + P_R \left|h_{RE}\right|^2 + P_I + N_0\right)}.$  The received signal at *p* can be written as  $y_p = Gh_{Ep}y_{E,2} + n_0.$  (17) Following the principle of SIC, the jamming signal is demodulated and deducted from superposition signal by p completely, before it demodulates its intended messages. The SINR for p to decode its own message is given by

$$\gamma_{p \to p} = \frac{P_S P_E |h_{Ep}|^2 |h_{SE}|^2}{P_R P_E |h_{Ep}|^2 |h_{RE}|^2 + P_E N_0 |h_{Ep}|^2 + P_S |h_{SE}|^2 N_0 + P_R |h_{RE}|^2 N_0 + P_I N_0 + N_0^2}$$
(18)

# Remarks:

(1) From the above description of the proposed protocol, we can see that in order to complete a secure communication, R needs to decode twice and recode once, m and p need to decode once and n needs to decode twice. The computational complexity of the proposed protocol is not very high.

(2) In our protocol, the source is responsible for the algorithm design. As there are only two relays in our system, common training processes of individual channels from source to relay and then to destination can be used to acquire the required CSI [28–30]. In addition, we use jamming not encryption in our protocol and no routing is required, so there is no overhead other than training processes.

# **3** Security performance analysis

In this section, we adopt EST as the metric of secrecy performance which considers the reliability performance and secrecy performance holistically. The exact EST expressions of m and n and approximate EST expression of p are derived in the following parts. The EST of m is expressed as

$$\eta_m = \tau_{m,s} \Pr\left(\gamma_{R \to m} > 2^{3\tau_{m,t}} - 1, \gamma_{m \to m} > 2^{3\tau_{m,t}} - 1, \gamma_{E \to m} < 2^{3(\tau_{m,t} - \tau_{m,s})} - 1\right),\tag{19}$$

where Pr (·) represents the probability that the expressions in brackets hold and  $\gamma_{E \to m}$  is expressed as

$$\gamma_{E \to m} = \max\left(\gamma_{E \to m, 1}, \gamma_{E \to m, 2}\right). \tag{20}$$

(20) indicates that the SINR of *E* wiretapping the message of *m* is the maximum eavesdropping SINR of the first time slot and the second time slot. Substituting (4), (6), (10) and (15) into (19), we can obtain

$$\Pr\left(\gamma_{R \to m} > 2^{3\tau_{m,t}} - 1, \gamma_{m \to p} > 2^{3\tau_{m,t}} - 1, \gamma_{E \to m} < 2^{3(\tau_{m,t} - \tau_{m,s})} - 1\right)$$

$$= \Pr\left(\frac{a_m |h_{SR}|^2 P_S}{a_n |h_{SR}|^2 P_S + N_0} > \theta_1, \frac{a_m |h_{Rm}|^2 P_R}{a_n |h_{Rm}|^2 P_R + N_0} > \theta_1, \left(21\right)\right)$$

$$\max\left(\frac{a_m P_S |h_{SE}|^2}{a_n P_S |h_{SE}|^2 + P_I + N_0}, \frac{a_m P_R |h_{RE}|^2}{a_n P_R |h_{RE}|^2 + P_I + N_0}\right) < \theta_2\right),$$

where  $\theta_1 = 2^{3\tau_{m,t}} - 1$  and  $\theta_2 = 2^{3(\tau_{m,t} - \tau_{m,s})} - 1$ . Following the channel assumption previously, we can get

$$Pr(\gamma_{R \to m} > \theta_{1}, \gamma_{m \to p} > \theta_{1}, \gamma_{E \to m} < \theta_{2})$$

$$= \exp \frac{-\lambda_{1}\theta_{1}}{(a_{m} - \theta_{1}a_{n})} \exp \frac{-\lambda_{4}\theta_{1}}{(a_{m} - \theta_{1}a_{n})}$$

$$\times \left(1 - \exp\left(\frac{-\lambda_{2}\theta_{2}(\rho_{I} + 1)}{(a_{m} - \theta_{2}a_{n})}\right)\right) \left(1 - \exp\left(\frac{-\lambda_{3}\theta_{2}(\rho_{I} + 1)}{P_{S}(a_{m} - \theta_{2}a_{n})}\right)\right),$$
(22)

where  $\rho_I = P_I/N_0$ . We have to notice that  $a_m - \theta_1 a_n > 0$  must be satisfied, if not,  $\eta_m$  will be zero. Submitting (22) into (19), we can get the closed-form EST expression of *m* which can be written as

$$\eta_m = \tau_{m,s} \exp \frac{-\lambda_1 \theta_1}{(a_m - \theta_1 a_n)} \exp \frac{-\lambda_4 \theta_1}{(a_m - \theta_1 a_n)} \times \left(1 - \exp\left(\frac{-\lambda_2 \theta_2(\rho_I + 1)}{(a_m - \theta_2 a_n)}\right)\right) \left(1 - \exp\left(\frac{-\lambda_3 \theta_2(\rho_I + 1)}{P_S(a_m - \theta_2 a_n)}\right)\right).$$
(23)

Similarly, the EST of *n* is expressed as

$$\eta_n = \tau_{n,s} \Pr\left(\gamma_{R \to m} > \theta_1, \gamma_{R \to n} > 2^{3\tau_{n,t}} - 1, \gamma_{n \to m} > \theta_1, \\ \gamma_{n \to n} > 2^{3\tau_{n,t}} - 1, \gamma_{E \to n} < 2^{3(\tau_{n,t} - \tau_{n,s})} - 1\right).$$

$$(24)$$

where  $\gamma_{E \to n} = \max (\gamma_{E \to n,1}, \gamma_{E \to n,2})$ . Similar to the analysis above, (24) can be expressed as

$$\eta_n = \tau_{n,s} \exp\left(-\lambda_1 g\right) \exp\left(-\lambda_4 g\right) \left(1 - \exp\left(\frac{-\lambda_2 \theta_4(\rho_I + 1)}{a_n}\right)\right) \\ \times \left(1 - \exp\left(\frac{-\lambda_3 \theta_4(\rho_I + 1)}{a_n}\right)\right),$$
(25)

where  $g = \max\left(\frac{\theta_1}{(a_m - \theta_1 a_n)}, \frac{\theta_3}{a_n}\right), \theta_3 = 2^{3\tau_{n,t}} - 1 \text{ and } \theta_4 = 2^{3(\tau_{n,t} - \tau_{n,s})} - 1.$ 

## 3.1 Approximate expression of p

The EST of p is expressed as

$$\eta_p = \tau_{p,s} \Pr\left(\gamma_{p \to p} > 2^{3\tau_{p,t}} - 1, \gamma_{E \to p} < 2^{3(\tau_{p,t} - \tau_{p,s})} - 1\right).$$
(26)

Before deriving the approximate expression of *p*, we set  $X = P_S |h_{SE}|^2 / N_0$ ,  $Y = P_E |h_{Ep}|^2 / N_0$  and  $Z = P_R |h_{RE}|^2 / N_0$ . According to (14) and (18), (26) can be rewritten as

$$\eta_p = \tau_{p,s} \Pr\left(\frac{XY}{YZ + X + Y + Z + \rho_I + 1} > \theta_5, \frac{X}{Z + \rho_I + 1} < \theta_6\right),\tag{27}$$

where  $\theta_5 = 2^{3\tau_{p,t}} - 1$  and  $\theta_6 = 2^{3(\tau_{p,t} - \tau_{p,s})} - 1$ . The first part in the brackets of (27) can be written as

$$X > \frac{\theta_5(Y + YZ + \rho_I + 1)}{Y - \theta_5}.$$
(28)

We have to notice that  $Y - \theta_5 > 0$  must be satisfied, if not,  $\eta_p$  will be zero. The second part in the brackets of (27) can be written as

$$X < \theta_6(Z + \rho_I + 1).$$
 (29)

With (28) and (29), we can get the bounds of *X* and according to the bounds,  $\frac{\theta_5(Y+YZ+\rho_I+1)}{Y-\theta_5} < \theta_6(Z+\rho_I+1)$ must be satisfied which can be rewritten as

$$((\theta_5 - \theta_6)Y + \theta_5\theta_6)Z < (\theta_6(\rho_I + 1) - \theta_5)Y - (\theta_5\theta_6 + \theta_5)(\rho_I + 1).$$
(30)

As  $((\theta_5 - \theta_6)Y + \theta_5\theta_6) > 0$  is always satisfied, we can get the bounds of *Z* as

$$0 < Z < \frac{(\theta_6(\rho_I + 1) - \theta_5)Y - (\theta_5\theta_6 + \theta_5)(\rho_I + 1)}{(\theta_5 - \theta_6)Y + \theta_5\theta_6}.$$
(31)

It is noticed that  $(\theta_6(\rho_I + 1) - \theta_5)Y - (\theta_5\theta_6 + \theta_5)(\rho_I + 1) > 0$  must be satisfied, if not,  $\eta_p$  will be zero. Then, we can get the bounds of *Y* as

$$Y > \frac{(\theta_5 \theta_6 + \theta_5)(\rho_I + 1)}{\theta_6(\rho_I + 1) - \theta_5}.$$
(32)

Compared (32) with the previous bound  $Y - \theta_5 > 0$ , we can easily get that (32) is the bond of *Y*. It is noticed that  $\theta_6(\rho_I + 1) - \theta_5 > 0$  must be satisfied in (32), or  $\eta_p = 0$ ; this inequality holds easily when  $\rho_I$  is large enough. Submitting the bounds expressions of (28), (29), (31) and (32) into (27), we can get the probability in (27) as

$$\Pr\left(\frac{XY}{YZ + X + Y + Z + \rho_I + 1} > \theta_5, \frac{X}{Z + \rho_I + 1} < \theta_6\right)$$
  
=  $\int_{\frac{(\theta_5 \theta_6 + \theta_5)(\rho_I + 1)}{\theta_6(\rho_I + 1) - \theta_5}}^{\infty} f(y) dy \int_0^{\frac{(\theta_6(\rho_I + 1) - \theta_5)y - (\theta_5 \theta_6 + \theta_5)(\rho_I + 1)}{(\theta_5 - \theta_6)y + \theta_5 \theta_6}} f(z) dz \int_{\frac{\theta_5(y + yz + \rho_I + 1)}{y - \theta_5}}^{\theta_6(z + \rho_I + 1)} f(x) dx.$ 
(33)

Following the channel assumption previously, we can get

$$\Pr\left(\frac{XY}{YZ + X + Y + Z + \rho_I + 1} > \theta_5, \frac{X}{Z + \rho_I + 1} < \theta_6\right)$$

$$= \lambda_3 \int_{\frac{(\theta_5\theta_6 + \theta_5)(\rho_I + 1)}{\theta_6(\rho_I + 1) - \theta_5}}^{\infty} f(y) dy \left[\frac{y - \theta_5}{(\lambda_3 + \lambda_2\theta_5)y - \lambda_3\theta_5}\right]$$

$$\times \left(1 - \exp\left(-\frac{((\lambda_3 + \lambda_2\theta_5)y - \lambda_3\theta_5)}{y - \theta_5}\frac{(\theta_6(\rho_I + 1) - \theta_5)y - (\theta_5\theta_6 + \theta_5)(\rho_I + 1)}{(\theta_5 - \theta_6)y + \theta_5\theta_6}\right)\right)\right)$$

$$\times \exp\left(\frac{-\lambda_2\theta_5(y + \rho_I + 1)}{y - \theta_5}\right) - \frac{1}{\lambda_3 + \lambda_2\theta_6}$$

$$\times \left(1 - \exp\left(-(\lambda_3 + \lambda_2\theta_6)\frac{(\theta_6(\rho_I + 1) - \theta_5)y - (\theta_5\theta_6 + \theta_5)(\rho_I + 1)}{(\theta_5 - \theta_6)y + \theta_5\theta_6}\right)\right)$$

$$\times \exp(-(\lambda_2\theta_6(\rho_I + 1)))].$$
(34)

When *Y* is large enough (in most cases, *Y* is very large because of the large jamming power), we can get  $((\lambda_3 + \lambda_2\theta_5)y - \lambda_3\theta_5)/y - \theta_5 \approx (\lambda_3 + \lambda_2\theta_5)$  and  $\frac{(\theta_6(\rho_I+1)-\theta_5)y-(\theta_5\theta_6+\theta_5)(\rho_I+1)}{(\theta_5-\theta_6)y+\theta_5\theta_6} \approx (\theta_6(\rho_I+1)-\theta_5)/(\theta_5-\theta_6)$ . Thus, invoking those two

approximations into (34) and with the help of [31, Equation (3.352.2)], (34) can be expressed as

$$\Pr\left(\frac{XY}{YZ + X + Y + Z + \rho_I + 1} > \theta_5, \frac{X}{Z + \rho_I + 1} < \theta_6\right)$$

$$\approx \frac{\lambda_3 \exp(-\lambda_2 \theta_5)}{(\lambda_3 + \lambda_2 \theta_5)} \left(1 - \exp\left(-\frac{(\lambda_3 + \lambda_2 \theta_5)(\theta_6(\rho_I + 1) - \theta_5)}{(\theta_5 - \theta_6)}\right)\right)$$

$$\times \left(\exp\left(-\frac{\lambda_6(\theta_5 \theta_6 + \theta_5)(\rho_I + 1)}{\theta_6(\rho_I + 1) - \theta_5}\right) + \left(\frac{\lambda_3 \theta_5}{(\lambda_3 + \lambda_2 \theta_5)} - \theta_5\right) \exp\left(-\frac{\lambda_3 \theta_5 \lambda_6}{(\lambda_3 + \lambda_2 \theta_5)}\right)$$

$$\times Ei\left(-\lambda_6 \frac{(\theta_5 \theta_6 + \theta_5)(\rho_I + 1)}{\theta_6(\rho_I + 1) - \theta_5} + \frac{\lambda_3 \theta_5 \lambda_6}{(\lambda_3 + \lambda_2 \theta_5)}\right)\right) - \frac{\lambda_3 \exp(-(\lambda_1 \theta_6(\rho_I + 1)))}{\lambda_3 + \lambda_2 \theta_6}$$

$$\times \left(1 - \exp\left(-(\lambda_3 + \lambda_2 \theta_6)\frac{(\theta_6(\rho_I + 1) - \theta_5)}{(\theta_5 - \theta_6)}\right)\right) \exp\left(-\frac{\lambda_6(\theta_5 \theta_6 + \theta_5)(\rho_I + 1)}{\theta_6(\rho_I + 1) - \theta_5}\right).$$
(35)

where  $Ei(\cdot)$  denotes the exponential integral function [31, Equation (8.211. 2)]. Submitting (35) into (27), we can get the approximate EST expression of p which can be expressed as

$$\eta_{p} \approx \tau_{m,s} \frac{\lambda_{3} \exp(-\lambda_{2}\theta_{5})}{(\lambda_{3} + \lambda_{2}\theta_{5})} \left(1 - \exp\left(-\frac{(\lambda_{3} + \lambda_{2}\theta_{5})(\theta_{6}(\rho_{I} + 1) - \theta_{5})}{(\theta_{5} - \theta_{6})}\right)\right)$$

$$\times \left(\exp\left(-\frac{\lambda_{6}(\theta_{5}\theta_{6} + \theta_{5})(\rho_{I} + 1)}{\theta_{6}(\rho_{I} + 1) - \theta_{5}}\right) + \left(\frac{\lambda_{3}\theta_{5}}{(\lambda_{3} + \lambda_{2}\theta_{5})} - \theta_{5}\right)\exp\left(-\frac{\lambda_{3}\theta_{5}\lambda_{6}}{(\lambda_{3} + \lambda_{2}\theta_{5})}\right)$$

$$\times Ei\left(-\lambda_{6}\frac{(\theta_{5}\theta_{6} + \theta_{5})(\rho_{I} + 1)}{\theta_{6}(\rho_{I} + 1) - \theta_{5}} + \frac{\lambda_{3}\theta_{5}\lambda_{6}}{(\lambda_{3} + \lambda_{2}\theta_{5})}\right)\right) - \frac{\lambda_{3}\exp(-(\lambda_{1}\theta_{6}(\rho_{I} + 1)))}{\lambda_{3} + \lambda_{2}\theta_{6}}$$

$$\times \left(1 - \exp\left(-(\lambda_{3} + \lambda_{2}\theta_{6})\frac{(\theta_{6}(\rho_{I} + 1) - \theta_{5})}{(\theta_{5} - \theta_{6})}\right)\right)\exp\left(-\frac{\lambda_{6}(\theta_{5}\theta_{6} + \theta_{5})(\rho_{I} + 1)}{\theta_{6}(\rho_{I} + 1) - \theta_{5}}\right).$$
(36)

# 4 Numerical results and discussion

In this section, computer simulations are performed to validate the above theoretical analysis. We introduce the channel model  $E(|h_{ij}|^2) = d_{ij}^{-\alpha}$ , where  $d_{ij}$  is the distance between node *i* and *j*, and  $\alpha = 3$  is the path loss exponent. The other parameters are set as follows:  $d_{SR} = 20$  m,  $d_{SE} = 30$  m,  $d_{RE} = 20$  m,  $d_{Rm} = 40$  m,  $d_{Rn} = 20$  m,  $d_{Ep} = 40$  m,  $R_{m,t} = R_{n,t} = 0.8$  bits/s/Hz,  $R_{p,t} = 0.4$  bits/s/Hz,  $R_{m,s} = R_{n,s} = 0.4$  bits/s/Hz,  $R_{p,s} = 0.2$  bits/s/Hz,  $a_m = 9/10$ ,  $a_n = 1/10$  and  $N_0 = -50$  dB.

Figure 2 illustrates the performance of the proposed scheme and HD-NOMA versus  $P_S$  with  $P_R = -18$  dB,  $P_I = 24$  dB and  $P_E = 15$  dB. The HD-NOMA system with two relays requires a total of 4 equal orthogonal time slots which is similar to [32]. The transmission detail of HD-NOMA is shown in Table 1. It can be observed that simulation and theoretical results match very well with each other for *m* and *n* and the approximate analysis for *p* is accurate because *Y* is very large in our setting which is very consistent with the actual communication scenario. Significantly, the EST of all users first increases and then decreases due to the increase of  $P_S$ , which demonstrates that increasing  $P_S$  cannot always improve EST as high  $P_S$  increases the risk



 Table 1
 Transmission of HD-NOMA

time slot	S	R	E	р
1	XS	_	_	<i>x</i> <sub>0</sub>
2	-	Xs	-	<i>x</i> 0
3	Хp			<i>x</i> 0
4	-	-	xp	-

of eavesdropping. It also shows that there exists an optimal  $P_S$  of our scheme to maximize EST for all users and this optimal value can easily be obtained by a onedimensional exhaustive search. Compared with HD-NOMA, the user p attains worse performance for any  $P_S$ , but one time slot can be saved in our scheme and this performance gap narrows when the optimal value of  $P_S$  is obtained. In addition, our scheme outperforms HD-NOMA for users m and n when  $P_S$  is small. All of the above statements illustrate the practical feasibility of our scheme.

Figure 3 shows the EST of users versus  $P_R$  with  $P_S = -6 \, dB$ ,  $P_I = 24 \, dB$  and  $P_E = 15 \, dB$ . For *m* and *n* of VFD-NOMA, it is shown that the analytical curves perfectly match the Monte Carlo simulation results and EST of *m* and *n* first increases and then decreases as high  $P_R$  increases the risk of eavesdropping for both two schemes. The optimal value of  $P_R$  to maximize the EST of *m* and *n* can also easily be obtained by a one-dimensional exhaustive search. For *p*, Fig. 3 confirms the close agreement between the simulation and approximate analytical results. We can also see that the performance of *p* in HD-NOMA does not affect by  $P_R$ , but the performance of *p* in our scheme decreases as  $P_R$  increases which is because  $P_R$  is considered as interference when *E* forwards the information of *p*. In addition, it is seen that when

 $P_R$  is small, the change of  $P_R$  does not affect the performance of p in our scheme. Although the existing HD-NOMA outperforms our protocol in some cases, our scheme can save one time slot and this performance gap is acceptable in actual communication scenario. Since the theoretical analyses agree well with the simulations, we will only plot the analytical results in the remaining figure.

Figure 4 plots the performance of our scheme and HD-NOMA versus  $P_I$  with  $P_S = -6 \text{ dB}$ ,  $P_R = -18 \text{ dB}$  and  $P_E = 15 \text{ dB}$ . We can observe that for *m* and *n*, increasing  $P_I$  can improve the EST, but 28dB is enough and no more power is needed. This result can help us saving interference signal power in actual communication scenario. We can also find that for *p*, increasing  $P_I$  cannot always improve EST as high  $P_I$  reduces the efficiency of the amplifier and the optimal value of  $P_I$  for *p* is basically the same as *m* and *n*.

## **5** Conclusion

In this paper, we studied the secrecy performance in VFD-NOMA networks. A VFD relaying scheme with an untrusted AF-HD relay and a trusted DF-HD relay is used in this system to improve the spectral efficiency where cooperative jamming is designed to confuse the untrusted relay. The exact and approximate expressions for EST are derived which shows that jamming is necessary for secure transmission and the powers of *S*, *R* and jamming should be carefully considered to improve secrecy performance and save the system energy consumption. From the simulation results, we can see that the proposed VFD-NOMA scheme is more practical than existing HD-NOMA scheme. As future work, the imperfect SIC receiver and adaptive power split factors can be further investigated.





#### Abbreviations

NOMA: Non-orthogonal multiple access; VFD: Virtual full-duplex; AF: Amplify-and-forward; HD: Half-duplex; DF: Decodeand-forward; EST: Effective secrecy throughput; OMA: Orthogonal multiple access; MIMO: Multiple-input multipleoutput; FD: Full-duplex; SI: Self-interference; CSI: Channel state information; SNR: Signal-to-noise ratio; SIC: Successive interference cancellation; SINR: Signal-to-interference-plus-noise ratio.

#### Acknowledgements

None.

#### Authors' contributions

WG proposed the system model, analyzed the performance and drafted the paper. YL participated in the simulations and helped to draft the manuscript. All authors read and approved the final manuscript.

#### Funding

None.

#### Availability of data and materials

Not available online. Please contact corresponding author for data requests.

#### Declarations

# Ethics approval and consent to participate

Not applicable.

## **Competing interests**

The authors declare that they have no competing interests.

#### Author details

<sup>1</sup>School of Information Science and Engineering, Shandong University, 72 Binhai Road, Jimo 266237, Qingdao, P. R. China. <sup>2</sup>School of Physics and Physical Engineering, Qufu Normal University, 57 Jingxuan West Road, Qufu 273165, Shandong, P. R. China. <sup>3</sup>State Grid Information and Telecommunication Group Co. Ltd., 1 Baiguang Road, Beijing 100192, China.

# Received: 21 February 2021 Accepted: 31 May 2021

Published online: 12 June 2021

#### References

- B. Selim, M.S. Alam, J.V.C. Evangelista, G. Kaddoum, B.L. Agba, NOMA-based IoT networks: impulsive noise effects and mitigation. IEEE Commun. Mag. 58, 69–75 (2020)
- M.S. Ali, E. Hossain, D.I. Kim, Coordinated multipoint transmission in downlink multi-cell NOMA systems: models and spectral efficiency performance. IEEE Wirel. Commun. 25, 24–31 (2018)
- 3. Z. Ding, H. Dai, H.V. Poor, Relay selection for cooperative NOMA. IEEE Wirel. Commun. Lett. 5, 416–419 (2016)

- 4. X. Pei, H. Yu, M. Wen, S. Mumtaz, S.A. Otaibi, M. Guizani, NOMA-based coordinated direct and relay transmission with a half-duplex/full-duplex relay. IEEE Trans. Commun. **68**, 6750–6760 (2020)
- Q. Wang, Y. Dong, X. Xu, X. Tao, Outage probability of full-duplex AF relaying with processing delay and residual selfinterference. IEEE Commun. Lett. 19, 783–786 (2015)
- 6. T. Kwon, S. Lim, S. Choi, D. Hong, Optimal duplex mode for DF relay in terms of the outage probability. IEEE Trans. Veh. Technol. **59**, 3628–3634 (2010)
- Z. Wei, X. Zhu, S. Sun, J. Wang, L. Hanzo, Energy-efficient full-duplex cooperative nonorthogonal multiple access. IEEE Trans. Veh. Technol. 67, 10123–10128 (2018)
- J. Jose, P. Shaik, V. Bhatia, VFD-NOMA under imperfect SIC and residual inter-Relay interference over generalized nakagami-m fading channels. IEEE Commun. Lett. 25, 646–650 (2021)
- M. Duarte, C. Dick, A. Sabharwal, Experiment-driven characterization of full-duplex wireless systems. IEEE Trans. Wirel. Commun. 11, 4296–4307 (2012)
- X. Yue, Y. Liu, S. Kang, A. Nallanathan, Z. Ding, Exploiting full/half duplex user relaying in NOMA systems. IEEE Trans. Commun. 66, 560–575 (2017)
- Q. Liau, C. Leow, Z. Ding, Amplify-and-forward virtual full-duplex relaying-based cooperative NOMA. IEEE Wirel. Commun. Lett. 7, 464–467 (2018)
- Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: technical challenges, recent advances, and future trends. Proc. IEEE 104, 1727–1765 (2016)
- J.T. Lim, K. Lee, Y. Han, Secure communication with outdated channel state information via untrusted relay capable of energy harvesting. IEEE Trans. Veh. Technol. 69, 11323–11337 (2020)
- A. Kuhestani, A. Mohammadi, P.L. Yeoh, Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer. IEEE Trans. Commun. 66, 2671–2684 (2018)
- M. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surv. Tutor. 16, 1550–1573 (2018)
- Y. Choi, J.H. Lee, A new cooperative jamming technique for a two-hop amplify-and-forward relay network with an eavesdropper. IEEE Trans. Veh. Technol. 67, 12447–12451 (2018)
- F. Ding, H. Wang, Y. Zhou, C. Zheng, Impact of relay's eavesdropping on untrusted amplify-and-forward networks over Nakagami-*m* fading. IEEE Wirel. Commun. Lett. 7, 102–105 (2018)
- C. Yuan, X. Tao, N. Li, W. Ni, R. Liu, P. Zhang, Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming. IEEE Trans. Veh. Technol. 68, 2682–2696 (2019)
- Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, M. Alouini, Secrecy analysis for cooperative NOMA networks with multiantenna full-duplex relay. IEEE Trans. Commun. 67, 5574–5587 (2019)
- A. Arafa, W. Shin, M. Vaezi, H.V. Poor, Secure relaying in non-orthogonal multiple access: trusted and untrusted scenarios. IEEE Trans. Inf. Forensics Secur. 15, 1–29 (2018)
- 21. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. 54, 1355–1387 (1975)
- 22. Z. Xiang, W. Yang, G. Pan, Y. Cai, X. Sun, Secure transmission in non-orthogonal multiple access networks with an untrusted relay. IEEE Wirel. Commun. Lett. **8**, 905–908 (2019)
- Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, L. Hanzo, Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. IEEE Trans. Wirel. Commun. 16, 1656–1672 (2017)
- Z. Han, N. Marina, M. Debbah, A. Hjrungnes, Physical layer security game: interaction between source, eavesdropper, and friendly jammer. EURASIP J. Wirel. Commun. Netw. 2009, 1–10 (2009)
- D. Fang, N. Yang, M. Elkashlan, P.L. Yeoh, J. Yuan, Cooperative jamming protocols in two hop amplify-and-forward wiretap channels, in *Proceedings of IEEE International Conference on Communications (ICC)*, June 9–13 2013; Budapest, Hungary, pp. 2188–2192 (2013)
- H. Zhang, H. Xing, J. Cheng, A. Nallanathan, V.C.M. Leung, Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming. IEEE Trans. Ind. Informat. 12, 1714–1725 (2016)
- R. Zhang, L. Song, Z. Han, B. Jiao, Physical layer security for two-way untrusted relaying with friendly jammers. IEEE Trans. Veh. Technol. 61, 3693–3704 (2012)
- F. Gao, T. Cui, A. Nallanathan, Optimal training design for channel estimation in decode-and-forward relay networks with individual and total power constraints. IEEE Trans. Signal Process. 56, 5937–5949 (2008)
- S. Zhang, F. Gao, C. Pei, X. He, Segment training based individual channel estimation in one-way relay network with power allocation. IEEE Trans. Wirel. Commun. 12, 1300–1309 (2013)
- G. Dou, X. He, R. Deng, J. Gao, Z. Cui, Individual channel estimation for AF-based relaying systems using in-band pilots. IEEE Commun. Lett. 20, 2201–2204 (2016)
- 31. I. Gradshteyn, I. Ryzhik, Table of Integrals, Series and Products (Academic Press, San Diego, 1994)
- J.B. Kim, I.H. Lee, Non-orthogonal multiple access in coordinated direct and relay transmission. IEEE Commun. Lett. 19, 2037–2040 (2015)

# Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.