Research Article

Impact of Antenna Selection on Physical-Layer Security of NOMA Networks

Dan Deng¹, Chao Li², Lisheng Fan², Xin Liu³, and Fasheng Zhou⁴

¹School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou, 511483, China

²School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China

³School of Information and Communication Engineering, Dalian University of Technology, China

⁴School of Physics and Electronic Engineering, Guangzhou University, Guangzhou 510006, China

Correspondence should be addressed to Lisheng Fan; lsfan@gzhu.edu.cn

Received 17 April 2018; Accepted 31 May 2018; Published 3 July 2018

Academic Editor: Li Sun

Copyright © 2018 Dan Deng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper studies the impacts of antenna selection algorithms in decode-and-forward (DF) cooperative nonorthogonal multiple access (NOMA) networks, where the secure information from the relay can be overheard by an eavesdropper in the networks. In order to ensure the secure transmission, an optimal antenna selection algorithm is proposed to choose one best relay's antenna to assist the secure transmission. We study the impact of antenna selection on the system secure communication through deriving the analytical expression of the secrecy outage probability along with the asymptotic expression in the high regime of signal-to-noise ratio (SNR) and main-to-eavesdropper ratio (MER). From the analytical and asymptotic expressions, we find that the system secure performance is highly dependent on the system parameters such as the number of antennas at the relay, SNR, and MER. In particular, the secrecy diversity order of the system is equal to the antenna number, when the interference from the second user is limited.

1. Introduction

In recent years, the wireless data rate has been explosively increasing [1–4], and many wireless services have been emerging, which requires the rapid development of wireless transmission [5–8]. As one of the most promising techniques, nonorthogonal multiple access (NOMA) provides superhigh data rate over the orthogonal multiple access, and hence it has been recognized as one candidate for the next-generation wireless communication networks [9, 10].

Moreover, NOMA has been demonstrated to be compatible with other emerging technologies [11–14]. In particular, the impact of imperfect self-interference cancellation for full-duplex cooperative NOMA is investigated in [12], while authors in [13] study the combination of NOMA and relay selection and results show that the proposed strategy can provide maximal diversity gain. Considering multiple sources, relay sharing scheme is proposed in [14] and results show that the proposed scheme outperforms OMA under perfect or imperfect SIC.

Due to the broadcast nature of wireless transmission, it is of vital importance to guarantee the transmission security from the application layer [15–19] to physical layer [20, 21]. The authors in [22] provided the framework of wiretap channels, which gives a general way to analyze and design the secure physical-layer security. In general, the performances of secure communications is affected by many wireless channel parameters, such as the channel correlation [23–25] and fading characteristics [26–28]. Recently, researchers turned to study the physical-layer security for NOMA communication systems. In [29], the authors proposed the transmission antenna selection for NOMA systems with multiple antennas, in order to ensure the secure communication. The authors in [30] optimized the secrecy sum rate of multiple users, in order to optimize the system design. Moreover, the authors in [31] investigated the downlink NOMA communication systems and proposed a secure beamforming algorithm to enhance the physical-layer security.

To further enhance the physical-layer security of NOMA systems, researchers proposed the spatial selection, such as

antenna selection or relay selection [32]. The authors in [33] extended this work into amplify-and-forward (AF) and decode-and-forward (DF) modes and devised a novel relay selection scheme which consists of two stages. The analytical results in this paper depicted that the proposed scheme outperformed the conventional relay selection schemes. The authors in [34] studied the NOMA system over Nakagami-m fading channels and verified that relay selection could enhance the wireless security for the fixed-gain relaying mode. In [13], the authors applied the relay selection technique into NOMA systems with multiple relays and demonstrated that the proposed scheme could achieve the maximum secrecy diversity gain. Moreover, the authors in [14] studied the NOMA systems with multiple sources, and devised a relay sharing scheme which was demonstrated to outperform the conventional OMA with either perfect or imperfect SIC. In [35], the authors studied the NOMA communication systems with AF relay, and derived the analytical outage expression for the cooperative NOMA networks.

However, as to the best of our knowledge, there are no literatures on the effects of the antenna selection algorithms on the secrecy outage probability for cooperative NOMA. Motivated by that, based on the optimal antenna selection algorithm, this paper studies the secrecy outage performance for decode-and-forward (DF) cooperative NOMA networks. (DF relay can decode the wireless signal before forwarding to the destination node, which can improve the link quality. While amplify-and-forward (AF) relay only amplifies its received signal and the link quality can not be improved. Considering the advantages of DF relay scheme compared with AF scheme, only DF cooperative network is studied in this paper.) By using NOMA protocol and with the help of the relay station, the source station transfers messages to two destinations simultaneously. The best antenna of relay is selected to assist the secure transmission from the source to the destinations. The impact of the system parameters is analyzed through deriving the exact analytical expressions on the secrecy outage performance as well as the asymptotic results with large SNR and main-to-eavesdropper ratio (MER). We find that the system secure performance is highly dependent on the system parameters such as the number of antennas at the relay, SNR, and MER. Specifically, the secrecy diversity order of the system is equal to the antenna number, when the interference from the second user is limited. Furthermore, simulation results are provided to validate the theoretical analysis.

The main contributions of this paper are summarized as follows:

- (1) An optimal antenna selection for cooperative NOMA networks is proposed and the closed-form exact expressions and the asymptotic expressions on the secrecy outage performance are derived.
- (2) According to the asymptotic analysis, the impacts of the system parameters on the secrecy outage probability are revealed. We find that, in the case of limited interference, the secrecy diversity order of the system is equal to the antenna number

FIGURE 1: Secure antenna selection for cooperative NOMA networks.

Notations. We use the notations $\log_2(\cdot)$ and $\ln(\cdot)$ to represent the logarithms with the base of 2 and natural, respectively. Moreover, we use notations $f_X(x)$ and $F_X(x)$ to represent the probability density function and cumulative distribution function of the random variable X , respectively. Notation $\mathbb{E}(X)$ returns the expectation result of a random event X . In addition, $x \sim \mathcal{CN}(\mu, \sigma^2)$ indicates that the random variable x follows a circularly symmetric complex-valued Gaussian distribution of the mean μ and variance σ^2 . We use the notation $R-D$ to denote the link from R to D .

2. System Model and Selection Algorithm

The system model of two-slot decode-and-forward (DF) cooperative NOMA networks is given in Figure 1. The considered system consists of one source station, a DF relay with N antennas, two destinations, and one passive eavesdropper, denoted as $S, R, \{D_1, D_2\}$, and E , respectively. The relay station is equipped with N antennas, and we use $\{R_n, n \in [1, N]\}$ to denote the n -th antenna of R . It is assumed that perfect channel status information (CSI) of $h_{SR_n}, h_{R_n D_1}$, and $h_{R_n D_2}$ can be obtained by the relay station through dedicated feedback channel [36–39]. Since the eavesdropper does not transmit any signal all the time [40], the relay cannot obtain the CSI of the eavesdropping links. Due to the long distance or severe shadow fading [41–43], there exists no direct link between the source and the destinations. Then with the assistant of the relay station, the source station can transfer messages to two destinations by using the NOMA protocol. Meanwhile, the wireless signal from the relay station may be intercepted by the eavesdropper. Both S and D are assumed to be equipped with a single antenna and operate in the half-duplex time-division mode. To reduce the information leakage to the eavesdropper, the *best* antenna in R is selected to decode the signal and forward to the destinations. As mentioned before, the destinations share the wireless channel through NOMA protocol. In addition, all of the wireless channels are assumed to be quasi-static Rayleigh block fading and statistically independent of each other.

In the first slot, a mixture signal is transmitted from the source station to the selected relay's antenna. Thus, the received signal at n -th antenna of R can be expressed as

$$r_{R_n} = h_{SR_n} \left(\sqrt{\alpha_1 P_S} x_1 + \sqrt{\alpha_2 P_S} x_2 \right) + n_{R_n}, \quad (1)$$

where x_1, x_2 are the messages transmitted from S to D_1 and D_2 , respectively. $n_{R_n} \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) received at R_n . We use P_S to denote the total transmission power of the source station and use $h_{SR_n} \sim \mathcal{CN}(0, \lambda_0)$ to represent the instantaneous channel fading coefficient between S and R_n . The power allocation factors for x_1 and x_2 are denoted by α_1, α_2 , respectively. According to the NOMA protocol [13], low rate and urgent traffic are carried by the first data stream, while the second data stream x_2 is used for opportunistic communications with long time tasks. To satisfy the total power requirement, α_1 and α_2 meet the following constraint: $\alpha_1 + \alpha_2 = 1$ and $\alpha_1 > \alpha_2$.

In this paper, we assume that perfect successive interference cancellation (SIC) receiver [44, 45] is used at R_n . Thus, x_2 is treated as interference before x_1 is decoded. Therefore, the SINRs for x_1 and x_2 at R_n can be obtained as

$$\text{SINR}_{R_n}^{(1)} = \frac{\alpha_1 P_S v_n}{\alpha_2 P_S v_n + \sigma^2}, \quad (2)$$

and

$$\text{SINR}_{R_n}^{(2)} = \frac{\alpha_2 P_S v_n}{\sigma^2}, \quad (3)$$

respectively, where $v_n = |h_{SR_n}|^2$ is used to denote the channel fading gain between S and R_n .

Consequently, the achievable rate for x_1 and x_2 at R_n can be expressed as follows:

$$\begin{aligned} C_{R_n}^{(1)} &= \frac{1}{2} \log_2 (1 + \text{SINR}_{R_n}^{(1)}) \\ &= \frac{1}{2} \log_2 \left(1 + \frac{\alpha_1 v_n}{\alpha_2 v_n + 1/\rho_S} \right), \end{aligned} \quad (4)$$

and

$$C_{R_n}^{(2)} = \frac{1}{2} \log_2 (1 + \text{SINR}_{R_n}^{(2)}) = \frac{1}{2} \log_2 (1 + \alpha_2 \rho_S v_n), \quad (5)$$

where $\rho_S = P_S/N_0$.

Both of the data streams, i.e., x_1 and x_2 , are decoded by the selected antenna in the second slot and forwarded to the destinations. Meanwhile, the wireless signal from the relay may be overheard by the passive eavesdropper. Given that R_n is selected and the received signal at D_2 and E can be given as

$$r_{D_2} = h_{R_n D_2} \left(\sqrt{\alpha_1 P_R} x_1 + \sqrt{\alpha_2 P_R} x_2 \right) + n_{D_2}, \quad (6)$$

$$r_E = h_{R_n E} \left(\sqrt{\alpha_1 P_R} x_1 + \sqrt{\alpha_2 P_R} x_2 \right) + n_E, \quad (7)$$

where $h_{R_n D_2} \sim \mathcal{CN}(0, \lambda_2)$, $h_{R_n E} \sim \mathcal{CN}(0, \lambda_E)$ are the instantaneous channel fading coefficient of R_n - D_2 and R_n - E links, respectively, P_R is the transmission power of R_n , $n_{D_2} \sim \mathcal{CN}(0, N_0)$, and $n_E \sim \mathcal{CN}(0, N_0)$ denote the AWGN received at D_2 and E , respectively.

Moreover, it is assumed that SIC receiver is used at both D_2 and E . That is, x_2 is treated as noise when they are trying

to decode x_1 . Thus, the achievable rates of x_1 at D_2 and E are given as (4)

$$C_{D_2}^{(1)} = \frac{1}{2} \log_2 (1 + \text{SINR}_{D_2}^{(1)}) \quad (8)$$

$$= \frac{1}{2} \log_2 \left(1 + \frac{\alpha_1 u_n}{\alpha_2 u_n + 1/\rho_R} \right),$$

$$C_E^{(1)} = \frac{1}{2} \log_2 (1 + \text{SINR}_E^{(1)}) \quad (9)$$

$$= \frac{1}{2} \log_2 \left(1 + \frac{\alpha_1 g_n}{\alpha_2 g_n + 1/\rho_R} \right),$$

where $u_n = |h_{R_n D_2}|^2$ and $g_n = |h_{R_n E}|^2$ denote the channel fading gain of links R_n - D_2 and R_n - E , respectively, and $\rho_R = P_R/N_0$.

Conditioned on that x_1 is decoded successfully, then the achievable rates of x_2 at D_2 and E can be expressed as

$$C_{D_2}^{(2)} = \frac{1}{2} \log_2 (1 + \text{SINR}_{D_2}^{(2)}) = \frac{1}{2} \log_2 (1 + \alpha_2 \rho_R u_n), \quad (10)$$

and

$$C_E^{(2)} = \frac{1}{2} \log_2 (1 + \text{SINR}_E^{(2)}) = \frac{1}{2} \log_2 (1 + \alpha_2 \rho_R g_n). \quad (11)$$

Thus, the secrecy capacity of the relaying system can be written as [46]

$$C_S = [C_{D_2}^{(2)} - C_E^{(2)}]^+, \quad (12)$$

where $[x]^+ = \max\{x, 0\}$.

Based on the theoretical analysis on the secrecy capacity, in order to minimize the secrecy outage probability of cooperative NOMA system, an optimal antenna selection algorithm is proposed in the following section.

The correctly decoding antenna subset is defined in the first step of the proposed algorithm as follows:

$$S_D = \{n : n \in [1, N], \text{SINR}_{R_n}^{(1)} \geq \gamma_1, \text{SINR}_{R_n}^{(2)} \geq \gamma_2\}, \quad (13)$$

with

$$\begin{aligned} \gamma_1 &= 2^{2R_1} - 1, \\ \gamma_2 &= 2^{2R_2} - 1, \end{aligned} \quad (14)$$

where R_1 and R_2 denote the minimum rate requirements for x_1 and x_2 , respectively.

It is easy to prove that both $C_{D_2}^{(1)}$ and $C_{D_2}^{(2)}$ are monotone increasing functions with respect to u_n . In the second step of the selection algorithm, since the relay has no CSI of the eavesdropper, the optimal antenna selection algorithm can be performed as follows:

$$n^* = \arg \max_{n \in S_D} \{u_n\}. \quad (15)$$

3. Performance Analysis

In this section, the theoretical analysis on the secrecy outage probability for the cooperative NOMA networks will be derived, as well as the asymptotic results. From the analysis, a deep insight on the effects of the system parameters, such as the antenna number and the power allocation factors, on the outage performance is present.

3.1. Exact Expression on Secrecy Outage Probability. In this section, the outage probability of the first step in (13) is analyzed. Given that relay antenna R_n is randomly selected, H_n is defined as the probability that R_n belongs to the decoding antenna subset S_D . By substituting (4) and (5) into (13), we have

$$\begin{aligned} H_n &= \Pr[R_n \in S_D] = \Pr[\text{SINR}_{R_n}^{(1)} \geq \gamma_1, \text{SINR}_{R_n}^{(2)} \geq \gamma_2] \\ &= e^{-c_3/\rho_S \lambda_0}, \end{aligned} \quad (16)$$

with

$$\begin{aligned} c_1 &= \frac{\gamma_1}{\alpha_1 - \alpha_2 \gamma_1}, \\ c_2 &= \frac{\gamma_2}{\alpha_2}, \\ c_3 &= \max\{c_1, c_2\}. \end{aligned} \quad (17)$$

Note that when $\gamma_1 \geq \alpha_1/\alpha_2$, no antenna can decode x_1 correctly, and the outage occurs definitely. Thus, we only need to consider the case that $\gamma_1 < \alpha_1/\alpha_2$.

We use $|S_D|$ to denote the size of subset S_D . Because of the statistical independence between $S - R_n$ links, the probability that $|S_D|$ equals M can be written as

$$\begin{aligned} \Pr\{|S_D| = M\} &= \binom{N}{M} (H_n)^M (1 - H_n)^{N-M} \\ &= \binom{N}{M} (e^{-c_3/\rho_S \lambda_0})^M (1 - e^{-c_3/\rho_S \lambda_0})^{N-M}. \end{aligned} \quad (18)$$

In particular, the outage probability that the size of S_D equals zero can be given as

$$\Pr[|S_D| = 0] = (1 - e^{-\gamma_m/\gamma_s \beta})^N. \quad (19)$$

We turn to consider the performance of the second step in (15), given that R_n is selected. The scenarios of successful secrecy transmission can be divided into two cases as follows. The first case is that both D_2 and E can decode x_1 successfully, and the secrecy capacity is better than the minimum requirement simultaneously. The probability of the first case can be given as

$$\begin{aligned} P_{n,1} &= \Pr[C_{D_2}^{(1)} \geq R_1, C_E^{(1)} \geq R_1, C_S \geq R_S] \\ &= \Pr[C_{D_2}^{(1)} \geq R_1, C_E^{(1)} \geq R_1, C_{D_2}^{(2)} - C_E^{(2)} \geq R_S]. \end{aligned} \quad (20)$$

By applying necessary mathematical derivation and substituting (8), (9), (10), and (11) into (20), we obtain

$$P_{n,1} = \Pr\left[u_n \geq g_n \gamma_S + \frac{c_4}{\rho_R}, g_n \geq \frac{c_1}{\rho_R}\right], \quad (21)$$

where $\gamma_S = 2^{2R_S}$ and $c_4 = (\gamma_S - 1)/\alpha_2$.

The second case is that E cannot decode x_1 correctly, but D_2 can. In this case, the secrecy capacity equals the achievable rate of x_2 at D_2 . The probability of the second case can be written as

$$P_{n,2} = \Pr[C_{D_2}^{(1)} \geq R_1, C_E^{(1)} < R_1, C_{D_2}^{(2)} \geq R_S]. \quad (22)$$

Similarly, substituting (8), (9), and (10) into (22), we obtain

$$P_{n,2} = \Pr\left[u_n \geq \frac{c_5}{\rho_R}, g_n < \frac{c_1}{\rho_R}\right]. \quad (23)$$

Using the full probability formula, the outage probability of this step can be calculated as

$$P_{O,n,M} = [1 - P_{n,1} - P_{n,2}], \quad (24)$$

where $M > 0$ is the size of the decoding antenna subset.

Thus, the secrecy outage probability of the cooperative NOMA system for R_n is

$$P_{O,n} = \Pr[|S_D| = 0] + \sum_{M=1}^N \Pr[|S_D| = M] P_{O,n,M}. \quad (25)$$

According to the order statistics [47], the CDF of u_{n^*} can be expressed as

$$F_{u_{n^*}}(x) = \Pr\{u_{n^*} < x\} = \Pr\{u_n < x, n \in S_D\}. \quad (26)$$

Due to the independence of channel fading gains u_n , the cumulative distribution function can be rewritten as

$$F_{u_{n^*}}(x) = \prod_{n=1}^M \Pr\{u_n < x\} = (1 - e^{-x/\lambda_2})^M. \quad (27)$$

By using the binomial theorem on (27), we obtain

$$F_{u_{n^*}}(x) = 1 - \sum_{k=1}^M \binom{M}{k} (-1)^{k-1} e^{-kx/\lambda_2}. \quad (28)$$

Using the analysis result in (28), the probability density function of u_{n^*} can be expressed as

$$f_{u_{n^*}}(x) = \sum_{k=1}^M \binom{M}{k} (-1)^{k-1} \frac{k}{\lambda_2} e^{-kx/\lambda_2}. \quad (29)$$

Since u_n is independent of g_n , the PDF of g_{n^*} remains the same with that of g_n ; i.e.,

$$f_{g_{n^*}}(x) = f_{g_n}(x) = \frac{1}{\lambda_E} e^{-x/\lambda_E}. \quad (30)$$

By applying (29) and (30) on (21) and (23), we have

$$P_{n^*,1} = \sum_{k=1}^M \binom{M}{k} \frac{(-1)^{k-1}}{c_{6,k} \lambda_E} e^{-c_{7,k}/\rho_R}, \quad (31)$$

with

$$\begin{aligned} c_{6,k} &= \frac{1}{\lambda_E} + \frac{k\gamma_S}{\lambda_2}, \\ c_{7,k} &= c_1 c_{6,k} + \frac{k c_4}{\lambda_2}, \end{aligned} \quad (32)$$

and

$$P_{n^*,2} = (1 - e^{-c_1/\rho_R \lambda_E}) \sum_{k=1}^M \binom{M}{k} (-1)^{k-1} e^{-k c_3/\rho_R \lambda_2}. \quad (33)$$

Using (31) and (33), $P_{O,n^*,M}$ in (24) and the secrecy outage probability in (25) for the optimal antenna selection can be expressed as in (34).

$$\begin{aligned} P_{O,n^*} &= \Pr\{|S_D| = 0\} + \sum_{M=1}^N \Pr\{|S_D| = M\} P_{O,n^*,M} \\ &= \Pr\{|S_D| = 0\} + \sum_{M=1}^N \Pr\{|S_D| = M\} \cdot \left\{ 1 \right. \\ &\quad \left. - \left[\sum_{k=1}^M \binom{M}{k} \frac{(-1)^{k-1}}{c_{6,k} \lambda_E} e^{-c_{7,k}/\rho_R} \right] \right. \\ &\quad \left. - \left[(1 - e^{-c_1/\rho_R \lambda_E}) \sum_{k=1}^M \binom{M}{k} (-1)^{k-1} e^{-k c_3/\rho_R \lambda_2} \right] \right\}. \end{aligned} \quad (34)$$

The details about the numerical computation and associated analysis can be found in the literature, such as the works [48–52] or [53–56].

3.2. Asymptotic Outage Probability Analysis. We present the asymptotic analysis in this section to reveal a deep insight on the effects of the system parameters on the outage probability. The asymptotic analysis focuses on the system behavior when the noise can be neglected. In this case, the main contribution or the bottleneck of the system performance can be revealed. Based on the asymptotic analysis, we can propose the optimization scheme on the system parameters. According to the asymptotic results, we can show behavior of the outage performance when both the transmission and the main-to-eavesdropper ratio (MER) are large enough.

Firstly, we give the definition of MER, which denotes the ratio of average fading power of $h_{R_n D_2}$ to that of $h_{R_n E}$; i.e.,

$$\mu = \frac{\lambda_2}{\lambda_E}. \quad (35)$$

Lemma 1. Given the definition of function $G(M, k) = \sum_{m=1}^M \binom{M}{m} (-1)^m m^k$, we have the following equation:

$$G(M, k) = 0, \quad \forall k = 1, 2, \dots, (M-1). \quad (36)$$

Proof. See Appendix A. $\square$

Lemma 2. Given the definition of function $A_N = \sum_{k=0}^N \binom{N}{k} ((-1)^k / (1 + k\delta))$, if $\delta \rightarrow 0$, we have the following approximation result:

$$A_N \approx (-\delta)^N G(N, N). \quad (37)$$

Proof. See Appendix B. $\square$

Consider the asymptotic expression of $P_{n^*,1}$ in (31). By using the approximation that $e^x = 1 + x$, we have

$$\begin{aligned} \hat{P}_{n^*,1} &= 1 - P_{n^*,1} \approx 1 - \sum_{k=1}^M \binom{M}{k} \frac{(-1)^{k-1}}{c_{6,k} \lambda_E} \left(1 - \frac{c_{7,k}}{\rho_R} \right) \\ &= 1 - \sum_{k=1}^M \binom{M}{k} \frac{(-1)^{k-1}}{1 + k(\gamma_S \lambda_E / \lambda_2)} \left(1 - \frac{c_{7,k}}{\rho_R} \right). \end{aligned} \quad (38)$$

Then, by using Lemma 2, we obtain

$$\begin{aligned} \hat{P}_{n^*,1} &= 1 - \sum_{k=1}^M \binom{M}{k} \frac{(-1)^{k-1}}{1 + k(\gamma_S \lambda_E / \lambda_2)} \left(1 - \frac{c_{7,k}}{\rho_R} \right) \\ &= \left(-\frac{\gamma_S}{\mu} \right)^M G(M, M) \\ &\quad + \sum_{k=1}^M \binom{M}{k} \frac{(-1)^k}{1 + k(\gamma_S / \mu)} \frac{c_{7,k}}{\rho_R} \\ &= \left(-\frac{\gamma_S}{\mu} \right)^M G(M, M) + \frac{c_1}{\rho_R \gamma_E}. \end{aligned} \quad (39)$$

Similarly, consider the asymptotic expression of $P_{n^*,2}$ in (33), and using the approximation $1 - e^{-x} = x$ yields

$$\begin{aligned} P_{n^*,2} &\approx \frac{c_1}{\rho_R \lambda_E} \sum_{k=1}^M \binom{M}{k} (-1)^{k-1} e^{-k c_3/\rho_R \lambda_2} \\ &\approx \left(\frac{c_1}{\rho_R \lambda_E} \right) \sum_{k=1}^M \binom{M}{k} (-1)^{k-1} \left(1 - \frac{k c_3}{\rho_R \lambda_2} \right) \\ &\approx \frac{c_1}{\rho_R \lambda_E} \sum_{k=1}^M \binom{M}{k} (-1)^{k-1} = \frac{c_1}{\rho_R \lambda_E}. \end{aligned} \quad (40)$$

When $\rho_S \rightarrow \infty$, the asymptotic result of (18) can be given as

$$\begin{aligned} \Pr\{|S_D| = M\} &\approx \binom{N}{M} \left(e^{-c_3/\rho_S \lambda_0} \right)^M \left(\frac{c_3}{\rho_S \lambda_0} \right)^{N-M} \\ &\approx \binom{N}{M} \left(\frac{c_3}{\rho_S \lambda_0} \right)^{N-M}. \end{aligned} \quad (41)$$

Specifically, when $M = 0$, we have

$$\Pr\{|S_D| = 0\} \approx \left(\frac{c_3}{\rho_S \lambda_0} \right)^N. \quad (42)$$

By substituting (39), (40), and (41) into (34), we can get the asymptotic expression on the outage probability

$$P_{O,n^*} = \left(\frac{c_3}{\rho_S \lambda_0} \right)^N + \sum_{M=1}^N \binom{N}{M} \left(\frac{c_3}{\rho_S \lambda_0} \right)^{N-M} \left(-\frac{\gamma_S}{\mu} \right)^M G(M, M). \quad (43)$$

Particularly, when the system is interference limited, i.e., $N_0 = 0$, we get

$$P_{O,n^*} \approx \sum_{M=1}^N \binom{N}{M} \left(\frac{c_3}{\rho_S \lambda_0} \right)^{N-M} \left(-\frac{\gamma_S}{\mu} \right)^M G(M, M) \approx \left(-\frac{\gamma_S}{\mu} \right)^N G(N, N). \quad (44)$$

From the asymptotic expression in (43) and (44), we can have the following remarks. (a) The asymptotic expression of the secrecy outage probability is jointly determined by the SNR, MER, and the antenna number. (b) For the interference limited system, the secrecy outage probability is only determined by the MER, and the diversity order of the outage probability equals the number of the antennas.

4. Simulation Results

In this section, we provide numerical results to verify the theoretical analysis, which shows the impacts of the system parameters, such as MER (μ), the number of antennas (N), the power allocation factor (α_1), and the rate requirement (R_S, R_2) on the secrecy outage probability as well as the asymptotic results. The Rayleigh fading channels are used in our simulation cases for all links in the NOMA relaying networks. Without loss of generality, in all simulation cases, we set that the transmission power of the relay is the same as that of the source station.

As a function of SNR (ρ_S), the effects of N on the outage probability is shown in Figure 2 with $\mu = 24$ dB. We set $\gamma_S = 60$ dB, $R_1 = R_2 = 1$ bps/Hz, $R_S = 0.1$ bps/Hz, and $\lambda_0 = 10$, and the antenna number changes from 1 to 3. From this figure, we can see that large N can introduce extra freedom the wireless fading channels, which can improve the outage probability with low SNR region. Also, when SNR grows to be large enough, an error floor occurs for the outage probability, which is determined by the MER and the antenna number. The reason is that when SNR approaches infinity, the bottleneck of the system performance is the interference introduced by NOMA protocol.

Figure 3 shows the effects of λ_0 on the outage probability as a function of SNR. The value of λ_0 changes from 1, 5 to 10. From this figure, we find that large λ_0 means that the average fading power of the first slot is large, which can obviously enlarge the size of the decoding antenna subset S_D . Thus, the secrecy outage probability can be reduced.

FIGURE 2: Secrecy outage probability versus SNR ρ_S with different N .

FIGURE 3: Secrecy outage probability versus SNR ρ_S with different λ_0 .

Figure 4 shows the effects of power allocation factor α_1 on the outage probability as a function of SNR. The value of α_1 changes as 0.8, 0.9, and 0.95. Under this configuration, we can see that small α_1 can get better system performance. The reason is that, in this case, the bottleneck is the capacity of data stream x_2 . Small α_1 means more power can be allocated for x_2 , which can improve the secrecy outage probability.

The effects of R_2 on the outage probability are depicted in Figure 5 with $R_S = 0.1$ bps/Hz as a function of SNR. The value of R_2 changes from 1.0 and 1.5 to 2.0 bps/Hz. Since small R_2

FIGURE 4: Secrecy outage probability versus SNR ρ_S with different α_1 .

FIGURE 5: Secrecy outage probability versus SNR ρ_S with different R_2 .

can enlarge the size of S_D , large freedom for the second hop can be obtained to improve the secure performance. Thus, we can see from the figure that small R_2 can significantly improve the outage performance.

As a function of MER μ , the analytical SOP in (34) and (44) for cooperative NOMA system is present in Figure 6. Considering the interference limited scenarios, we set $\gamma_S = 60$ dB, $R_1 = R_2 = 1$ bps/Hz, $R_S = 0.1$ bps/Hz, and $\lambda_0 = 10$, and the number of antennas N increases from 1 to 3. From this figure, it is seen that the analytical SOP curves match the simulation SOP curves well in all regions, while, in the high

FIGURE 6: Secrecy outage probability versus MER μ .

FIGURE 7: Secrecy outage probability versus SNR ρ_S with different μ .

SNR region, the simulation SOP curves converge to that of the asymptotic line. The accuracy of the theoretical analysis can be verified in all the simulation cases. Furthermore, we find that the diversity order of the outage probability is equal to the number of the antennas.

The effects of μ on the outage probability with $N = 2$ is shown in Figure 7. We can see that, in high SNR region, all lines approach an error floor, and small μ results in worse outage performance. The reason is that μ denotes the average fading power of the main-to-eavesdropper ration, and large μ can lower the outage probability of the system.

FIGURE 8: Secrecy outage probability versus SNR ρ_S with different R_S .

Figure 8 shows the effects of R_S on the outage probability with $\mu = 24$ dB as a function of SNR. The other parameters are set as the same as Figure 7. The value of R_S is set as 0.1 and 0.4. We can see from the figure that small R_S can lower the outage probability, which is consistent with intuition.

5. Conclusion

In this paper, we propose an optimal antenna selection algorithm to enhance the secure performance for DF cooperative NOMA networks. The exact analytical expressions on the secrecy outage performance are derived, as well as the asymptotic results in the high regime of signal-to-noise ratio (SNR) and main-to-eavesdropper ratio (MER). From the analytical and asymptotic expressions, we find that the system secure performance is highly dependent on the system parameters such as the number of antennas at the relay, SNR, and MER. Specifically, the secrecy diversity order of the system is equal to the antenna number, when the interference from the second user is limited. In the future works, we will incorporate other wireless transmission techniques such as the works in [57–61], in order to further enhance the system performance and ensure the secure communications.

Appendix

A. Proof of Lemma 1

Considering the definition of $G(M, k)$, by using the binomial theorem, we can easily find that $G(M, 0) = -1$. Applying variable substitution on $G(M, 1)$, we have

$$\begin{aligned} G(M, 1) &= \sum_{m=1}^M \binom{M}{m} (-1)^m m \\ &= -M \sum_{m=1}^M \binom{M-1}{m-1} (-1)^{m-1} \\ &= -M \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m = 0. \end{aligned} \quad (\text{A.1})$$

Similarly, we can prove $G(M, 2) = 0$.

Generally, consider the definition of $G(M, k)$, and we have

$$\begin{aligned} G(M, k) &= \sum_{m=1}^M \binom{M}{m} (-1)^m m^k \\ &= -M \sum_{m=1}^M \binom{M-1}{m-1} (-1)^{m-1} m^{k-1} \\ &= -M \sum_{m=1}^M \binom{M-1}{m-1} (-1)^{m-1} (m-1+1)^{k-1}. \end{aligned} \quad (\text{A.2})$$

By applying binomial theorem on $G(M, k)$, we have

$$\begin{aligned} G(M, k) &= -M \sum_{m=1}^M \binom{M-1}{m-1} (-1)^{m-1} \\ &\quad \cdot \left[1 + \sum_{j=1}^{k-1} \binom{k-1}{j} (m-1)^j \right] \\ &= -M \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m \left[1 + \sum_{j=1}^{k-1} \binom{k-1}{j} (m)^j \right] \\ &= -M \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m \sum_{j=1}^{k-1} \binom{k-1}{j} (m)^j \\ &= -M \sum_{j=1}^{k-1} \sum_{m=1}^{M-1} \binom{M-1}{m} (-1)^m \binom{k-1}{j} m^j \\ &= -M \sum_{j=1}^{k-1} \binom{k-1}{j} G(M-1, j). \end{aligned} \quad (\text{A.3})$$

Since $G(M, 1) = G(M, 2) = 0$, according to (A.3), we obtain $G(M, 3) = 0$. Furthermore, with mathematical induction, we can prove that $G(M, k) = 0, \forall k = 1, 2, \dots, (M-1)$.

Lemma 1 is proved.

B. Proof of Lemma 2

Proof. For $x \rightarrow 0$, using the series expansion equation that $1/(1+x) = \sum_{m=0}^{\infty} (-1)^m x^m$, we have

$$\begin{aligned} A_N &= \sum_{k=0}^N \binom{N}{k} \frac{(-1)^k}{1+k\delta} \\ &= \sum_{k=0}^N \binom{N}{k} (-1)^k \sum_{m=0}^{\infty} (-1)^m (k\delta)^m \quad (\text{B.1}) \\ &= \sum_{m=0}^{\infty} (-\delta)^m \sum_{k=0}^N \binom{N}{k} (-1)^k k^m. \end{aligned}$$

By using Lemma 1, we have

$$\begin{aligned} A_N &= \sum_{m=0}^{\infty} (-\delta)^m \sum_{k=1}^N \binom{N}{k} (-1)^k k^m \quad (\text{B.2}) \\ &= \sum_{m=0}^{\infty} (-\delta)^m G(N, m). \end{aligned}$$

Since $\delta \rightarrow 0$, we can ignore the high order items. Thus, A_N can be rewritten as

$$A_N \approx (-\delta)^N G(N, N). \quad (\text{B.3})$$

Lemma 2 is proved. $\square$

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Scientific Research Project of Education Department of Guangdong, China, under Grant 2017GKTSCX045, in part by the Science and Technology Program of Guangzhou, China, under Grant 201707010389, 201807010103 and 201804010127, in part by the Scientific Research Project of Guangzhou Municipal University under Grant 1201620439, in part by the Qingshanhu Young Scholar Program in GZPYP under Grant 2016Q001, and in part by Comba Research Funds under Grant H2017007, in part by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2014A030306027, in part by the Innovation Team Project of Guangdong Province University under Grant 2016KCXTD017.

References

[1] G. Huang, Q. Zhang, and J. Qin, "Joint Time Switching and Power Allocation for Multicarrier Decode-and-Forward Relay

Networks with SWIPT," *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2284–2288, 2015.

- [2] H. Marshoud, P. C. Sofotasios, S. Muhaidat, G. K. Karagiannidis, and B. S. Sharif, "On the Performance of Visible Light Communication Systems with Non-Orthogonal Multiple Access," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6350–6364, 2017.
- [3] X. Liu, F. Li, and Z. Na, "Optimal Resource Allocation in Simultaneous Cooperative Spectrum Sensing and Energy Harvesting for Multichannel Cognitive Radio," *IEEE Access*, vol. 5, pp. 3801–3812, 2017.
- [4] M. Shirvanimoghaddam, M. Condoluci, M. Dohler, and S. J. Johnson, "On the Fundamental Limits of Random Non-Orthogonal Multiple Access in Cellular Massive IoT," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2238–2252, 2017.
- [5] G. Liu, H. Liu, H. Chen, C. Zhou, and L. Shu, "Position-based adaptive quantization for target location estimation in wireless sensor networks using one-bit data," *Wireless Communications and Mobile Computing*, vol. 16, no. 8, pp. 929–941, 2016.
- [6] G. Huang and D. Tang, "Wireless Information and Power Transfer in Two-Way OFDM Amplify-and-Forward Relay Networks," *IEEE Communications Letters*, vol. 20, no. 8, pp. 1563–1566, 2016.
- [7] W. Tan, M. Matthaiou, S. Jin, and X. Li, "Spectral Efficiency of DFT-Based Processing Hybrid Architectures in Massive MIMO," *IEEE Wireless Communications Letters*, 2017.
- [8] X. Liu, X. Zhang, M. Jia, L. Fan, W. Lu, and X. Zhai, "5G-based green broadband communication system design with simultaneous wireless information and power transfer," *Physical Communication*, vol. 28, pp. 130–137, 2018.
- [9] Z. Ding, P. Fan, and H. V. Poor, "Random Beamforming in Millimeter-Wave NOMA Networks," *IEEE Access*, vol. 5, pp. 7667–7681, 2017.
- [10] J. Li, X. Jiang, Y. Yan, W. Yu, S. Song, and M. H. Lee, "Low Complexity Detection for Quadrature Spatial Modulation Systems," *Wireless Personal Communications*, vol. 95, no. 4, pp. 4171–4183, 2017.
- [11] J.-B. Kim and I.-H. Lee, "Non-orthogonal multiple access in coordinated direct and relay transmission," *IEEE Communications Letters*, vol. 19, no. 11, pp. 2037–2040, 2015.
- [12] C. Zhong and Z. Zhang, "Non-Orthogonal Multiple Access with Cooperative Full-Duplex Relaying," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2478–2481, 2016.
- [13] Z. Ding, H. Dai, and H. V. Poor, "Relay Selection for Cooperative NOMA," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 416–419, 2016.
- [14] M. F. Kader, M. B. Shahab, and S. Y. Shin, "Exploiting Non-Orthogonal Multiple Access in Cooperative Relay Sharing," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1159–1162, 2017.
- [15] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Information Sciences*, vol. 412–413, pp. 223–241, 2017.
- [16] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing," *Knowledge-Based Systems*, vol. 79, pp. 18–26, 2015.
- [17] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private Naive Bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89–104, 2018.

- [18] J. Li, X. Chen, X. Huang et al., "Secure distributed deduplication systems with improved reliability," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 64, no. 12, pp. 3569–3579, 2015.
- [19] J. Li, X. Chen, S. S. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," *Journal of Network and Computer Applications*, vol. 112, pp. 89–96, 2018.
- [20] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying with Cochannel Interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.
- [21] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 21879–21887, 2018.
- [22] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [23] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.
- [24] H. Xu, L. Sun, P. Ren, Q. Du, and Y. Wang, "Cooperative Privacy Preserving Scheme for Downlink Transmission in Multiuser Relay Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 825–839, 2017.
- [25] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying over Correlated Fading Channels," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 2811–2820, 2017.
- [26] G. Pan, H. Lei, Y. Deng et al., "On Secrecy Performance of MISO SWIPT Systems with TAS and Imperfect CSI," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3831–3843, 2016.
- [27] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Communications*, vol. 14, no. 12, pp. 1–14, 2017.
- [28] R. Zhao, Y. Yuan, L. Fan, and Y.-C. He, "Secrecy Performance Analysis of Cognitive Decode-and-Forward Relay Networks in Nakagami-m Fading Channels," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2017.
- [29] H. Lei, J. Zhang, K.-H. Park et al., "On Secure NOMA Systems with Transmit Antenna Selection Schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.
- [30] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930–933, 2016.
- [31] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure Beam-forming in Downlink MISO Nonorthogonal Multiple Access Systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7563–7567, 2017.
- [32] D. Deng, L. Fan, X. Lei, W. Tan, and D. Xie, "Joint user and relay selection for cooperative NOMA networks," *IEEE Access*, vol. 2017, no. 5, pp. 20220–20227, 2017.
- [33] Z. Yang, Z. Ding, Y. Wu, and P. Fan, "Novel relay selection strategies for cooperative NOMA," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 99, pp. 10114–10123, 2017.
- [34] X. Yue, Y. Liu, S. Kang, and A. Nallanathan, "Performance Analysis of NOMA with Fixed Gain Relaying over Nakagami-m Fading Channels," *IEEE Access*, vol. 5, pp. 5445–5454, 2017.
- [35] X. Liang, Y. Wu, D. W. K. Ng, Y. Zuo, S. Jin, and H. Zhu, "Outage Performance for Cooperative NOMA Transmission with an AF Relay," *IEEE Communications Letters*, vol. 21, no. 11, pp. 2428–2431, 2017.
- [36] W. Tan, S. Jin, C. Wen, and T. Jiang, "Spectral efficiency of multi-user millimeter wave systems under single path with uniform rectangular arrays," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, 2017.
- [37] X. Liu, M. Jia, X. Gu, and X. Tan, "Optimal periodic cooperative spectrum sensing based on weight fusion in cognitive radio networks," *Sensors*, vol. 13, no. 4, pp. 5251–5272, 2013.
- [38] G. Huang and W. Tu, "Optimal resource allocation in wireless-powered OFDM relay networks," *Computer Networks*, vol. 104, pp. 94–107, 2016.
- [39] D. Deng, M. Yu, J. Xia, Z. Na, J. Zhao, and Q. Yang, "Wireless powered cooperative communications with direct links over correlated channels," *Physical Communication*, vol. 28, pp. 147–153, 2018.
- [40] J. Li, M. Wen, X. Jiang, and W. Duan, "Space-Time Multiple-Mode Orthogonal Frequency Division Multiplexing with Index Modulation," *IEEE Access*, vol. 5, pp. 23212–23222, 2017.
- [41] X. Wang, H. Zhang, L. Fan, and Y. Li, "Performance of Distributed Switch-and-Stay Combining for Cognitive Relay Networks with Primary Transceiver," *Wireless Personal Communications*, vol. 97, no. 2, pp. 3031–3042, 2017.
- [42] X. Liu, M. Jia, X. Gu, J. Yan, and J. Zhou, "Optimal spectrum sensing and transmission power allocation in energy-efficiency multichannel cognitive radio with energy harvesting," *International Journal of Communication Systems*, vol. 30, no. 5, p. e3044, 2017.
- [43] J. Yuan, S. Jin, W. Xu, W. Tan, M. Matthaiou, and K.-K. Wong, "User-Centric Networking for Dense C-RANs: High-SNR Capacity Analysis and Antenna Selection," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 5067–5080, 2017.
- [44] X. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-Enhancing Scheme for Spatial Modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2018.
- [45] G. Huang and W. Tu, "Wireless Information and Energy Transfer in Nonregenerative OFDM AF Relay Systems," *Wireless Personal Communications*, vol. 94, no. 4, pp. 3131–3146, 2017.
- [46] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [47] H. A. David and H. N. Nagaraja, *Order Statistics*, Wiley Online Library, 3rd edition, 2003.
- [48] H. Wu, Y. Liao, Y. Ding, H. Wang, C. Peng, and S. Yin, "Engineering thermal and mechanical properties of multilayer aligned fiber-reinforced aerogel composites," *Heat Transfer Engineering*, vol. 35, no. 11-12, pp. 1061–1070, 2014.
- [49] J. Deng, Z. John Ma, A. Liu, S. Cao, and B. Zhang, "Seismic Performance of Reinforced Concrete Bridge Columns Subjected to Combined Stresses of Compression, Bending, Shear, and Torsion," *Journal of Bridge Engineering*, vol. 22, no. 11, p. 04017099, 2017.
- [50] Y. Liang, H. Wu, G. Huang, J. Yang, and H. Wang, "Thermal performance and service life of vacuum insulation panels with aerogel composite cores," *Energy and Buildings*, vol. 154, pp. 606–617, 2017.
- [51] J. Deng, A. Liu, Q. Yu, and G. Peng, "Seismic performances of steel reinforced concrete bridge piers," *Steel and Composite Structures*, vol. 21, no. 3, pp. 661–677, 2016.
- [52] J. Yang, H. Wu, M. Wang, and Y. Liang, "Prediction and optimization of radiative thermal properties of nano TiO2

- assembled fibrous insulations,” *International Journal of Heat and Mass Transfer*, vol. 117, pp. 729–739, 2018.
- [53] J. Yang, H. Wu, M. Wang, S. He, and H. Huang, “Prediction and optimization of radiative thermal properties of ultrafine fibrous insulations,” *Applied Thermal Engineering*, vol. 104, pp. 394–402, 2016.
- [54] J. Deng, A. Liu, P. Huang, and X. Zheng, “Interfacial mechanical behaviors of RC beams strengthened with FRP,” *Structural Engineering and Mechanics*, vol. 58, no. 3, pp. 577–596, 2016.
- [55] J. Yang, H. Wu, S. He, and M. Wang, “Prediction of thermal conductivity of fiber/aerogel composites for optimal thermal insulation,” *Journal of Porous Media*, vol. 18, no. 10, pp. 971–984, 2015.
- [56] J. Deng, A. Liu, Z. Ma, P. Huang, and R. Zhou, “Interfacial behavior of RC beams strengthened with FRP under fatigue loading,” *Advances in Structural Engineering*, vol. 18, no. 2, pp. 283–293, 2015.
- [57] J. Xia, F. Zhou, X. Lai et al., “Cache Aided Decode-and-Forward Relaying Networks: From the Spatial View,” *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 5963584, 9 pages, 2018.
- [58] X. Liu, Y. Wang, Y. Chen et al., “A Multichannel Cognitive Radio System Design and Its Performance Optimization,” *IEEE Access*, vol. 6, pp. 12327–12335, 2018.
- [59] F. Shi, L. Fan, X. Liu, Z. Na, and Y. Liu, “Probabilistic Caching Placement in the Presence of Multiple Eavesdroppers,” *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 2104162, 10 pages, 2018.
- [60] X. Liu, M. Jia, X. Gu, F. Kong, and Q. Jing, “Optimal joint allocation of multislot spectrum sensing and transfer power in multichannel cognitive radio,” *Journal of Sensors*, vol. 2014, Article ID 2104162, 9 pages, 2014.
- [61] F. Zhou, L. Fan, X. Lei, G. Luo, H. Zhang, and J. Zhao, “Edge Caching With Transmission Schedule for Multiuser Multirelay Networks,” *IEEE Communications Letters*, vol. 22, no. 4, pp. 776–779, 2018.