Covert Non-Orthogonal Multiple Access Communication Assisted by Multi-Antenna Jamming

Noname manuscript No.
(will be inserted by the editor)

Covert Non-Orthogonal Multiple Access Communication Assisted by Multi-Antenna Jamming

Hongxing Peng · Wenjing He · Yanliang Zhang · Xingwang Li · Yuan Ding · Varun G Menon · Sandeep Verma

Received: date / Accepted: date

Abstract As the Internet of Things (IoT) becomes increasingly popular, the amount of information transmitted through the IoT network has increased significantly. Therefore, the privacy and security problem of the transmitted information has become a major area of focus. Motivated by this, this paper considers the covert communication based on non-orthogonal multiple access (NOMA), which consists of a transmitter, a legal user, a warden with power detection function and a multi-antenna jammer. To realize the covert communication between the transmitter and the legitimate user, the detection error probability of the warden is firstly derived, and then the optimal detection threshold and the minimum detection error probability (MDEP) are obtained. In addition, with the aim of designing this system, the average MDEP of the warden is calculated, and the closed form solution for the outage probability (OP) of the communication link is obtained. Then, a scheme is proposed to optimize the covertness of this system under the covertness constraint and interruption constraint, through which the maximum covert throughput of the

Hongxing Peng · Wenjing He · Yanliang Zhang · Xingwang Li
School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454000, China
E-mail: {phx, Ylzhang, lixingwang}@hpu.edu.cn, hewenjing07@163.com

Yuan Ding
School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, Scotland, UK
E-mail: yuan.ding@hw.ac.uk

Varun G Menon
Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, India
E-mail: varungmenon46@gmail.com

Sandeep Verma
Department of Electronics and Communication Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar-144011, India
E-mail: sandeepv.ec.13@nitj.ac.in

system can be obtained. The simulated numerical results validate the theoretical analysis, and testify that: *i*) the detection performance of the warden can be reduced by increasing the maximum jamming power of the jammer or reducing the transmitting power of the transmitter; *ii*) by optimizing the power allocation factor, the maximum covert throughput of the system can be obtained under the premise of satisfying the covertness constraint and interruption condition; *iii*) the proposed optimization scheme can enhance the covertness performance of this system.

Keywords Covert communication · covert throughput · detection error probability · NOMA · random power

1 Introduction

With the rapid development of mobile communication technology, data traffic is growing exponentially [1]. In the meantime, wireless communication operators are faced with a huge challenge of managing the limited spectrum resources to meet the ubiquitous connection demand. Therefore, improving the utilization of spectrum resources has become a key research direction in academia and industry [2]. In orthogonal multiple access (OMA) technologies [3], a user can only be allocated a single wireless resource, such as dividing the wireless resources according to frequency or time. Consequently, due to the shortage of spectrum resources, OMA technologies are unable to meet the future communication requirements of high rate, diverse quality of services, low-latency and massive connections [4]. Therefore, non-orthogonal multiple access (NOMA) has been proposed as a promising technology for the fifth generation (5G) wireless network [5–10]. At present, the mainstream scheme of NOMA is to achieve signal multiplexing in power domain (PD) or code domain (CD) [11,12].

In NOMA, the transmitters send the superposition signal, and the receivers recover their own signal by decoding the superposition signal using successive interference cancellation (SIC) [13–17]. Moreover, NOMA technologies allow all service users enjoy the same time, frequency and code resource block through power multiplexing. In addition, NOMA can also allocate different power to users with different channel conditions, which ensures fairness between users. Given this fact, NOMA has been extensively studied in wireless communication. In [18], Huang *et al.* discussed a cooperative relay network based on dual-hop NOMA, and derived the form of closed solutions of the outage probability (OP) for decode-and-forward and amplify-and-forward protocols. Considering the use of instantaneous channel state information (CSI) in the user ordering, Li *et al.* [19] proposed a new two-stage relay selection scheme, obtaining the analytical expressions for the OP and the diversity order of the proposed scheme. The authors of [20] investigated the cooperative NOMA system with energy collection function in the multi-cell network, and analyzed its coverage probability, ergodic rate and energy efficiency. From the

viewpoint of a unified NOMA framework, the authors in [21] studied the secrecy behavior in different eavesdropping scenarios, while derived the exact and asymptotic expressions of the secrecy OP of CD/PD-NOMA and imperfect/perfect SIC to characterize the secrecy performance. A new co-operative simultaneous wireless information and power transfer NOMA protocol was proposed in [22], where the near user acted as an energy collecting relay to assist the far user. Yin *et al.* [23] proposed a dynamic user grouping algorithm to classify users, and compared the performance of NOMA-2000 and PD-NOMA with Rayleigh fading channels.

Due to the broadcast nature of wireless transmission, the security problem has been a great challenge, and no exception for the NOMA system. For the purpose of ensuring the integrity of information, traditional security technology adopts encryption to prevent eavesdropping [24]. However, studies in recent years have shown that many traditional encryption methods are no longer reliable with the constant improvement of computation capability [25]. In view of this fact, some research works have investigated such security problems from the aspect of physical layer security (PLS) [26–32]. However, the whole research of PLS is mainly paid attention to protecting the content of communication. Furthermore, in addition to the security of information, users also aim to hide their communication behaviors from being detected by the monitors in certain communication scenarios (such as military activities, remote health monitoring, etc.). Based on this background, a new security mode has emerged, which is called covert communication [33,34]. Covert communication not only prevents the content of the communication from being eavesdropped, but also ensures the transmission between the two parties is non-detected by eavesdroppers.

Covert communication is designed to ensure that when wireless signals are transmitted and/or communication behaviors are performed, the signals and/or behaviors have a higher detection error probability at the warden. In recent years, covert communication has aroused extensive research interest and become a cutting-edge technology in the field of secure communication [35–42]. In [35], Liu *et al.* proved that wireless communication can be hidden in the interference of noisy wireless networks, and discussed some new results on the active wiretapping effect. The authors of [36] studied the performance of covert communication in multiple relays-assisted IoT systems and proposed two relay selection schemes based on random selection and superior-link selection. Shmuel *et al.* [37] investigated the situation in which the jammer is configured with multi-antenna, and analyzed the transmission strategy at the jammer that affects the transmission rate in the case of full CSI and partial CSI. In [38], Hu *et al.* proposed truncated channel inversion power control (CIPC) scheme to realize covert communication, analyzed the Willie's detection performance limits of the proposed scheme and traditional CIPC scheme, and obtained the effective covert throughputs. Shahzad *et al.* [39] proposed to adopt the full-duplex (FD) receiver to realize covert communication, and derived the form of closed solution of the average optimal detection probability at Willie. In [40], Xiong *et al.* studied covert communication on additive

white Gaussian noise (AWGN) channels with the help of cognitive jammer, and showed that the cognitive jammer brought covert rate gain over the non-informed jammer. The authors in [41] and [42] studied a covert communication system over a packet fading channel where the transceiver is uncertain about the relevant CSI.

The above describes some related researches on covert communication. However, to the best of our knowledge, there are few articles about covert communication combined with NOMA. The only related research works can be found in [43–45]. In uplink NOMA systems, the authors of [43] proposed the adoption of CIPC in the public communication link to make full use of the channel uncertainty to realize covert communication. In [44], Jiang *et al.* designed a cooperative covert communication scheme using cellular and non-cellular signals, and used the PD-NOMA to decode the covert message. In downlink NOMA systems, Tao *et al.* [45] used open legal communication to provide cover for covert communication, derived detection error probability and connect outage probabilities of Willie, and optimized the PAF ratio to maximize the effective covert rate.

1.1 Motivation and Contributions

Driven by the above discussion, we find that the existing literature often only focuses on the transmission of a single covert message in terms of covert communication. However, with the rapid development of communication technology, multi-task communication scenarios will gradually become the mainstream. Secondly, the combination of covert communication and NOMA can not only meet the covertness of the system and realize covert communication, but also improve the transmission rate of information, so as to further improve the system performance. Regarding to the combination of NOMA and covert communication, signals sent by single antenna are often used as interference signals, but most antennas in real life are multi-antenna. Therefore, we study the influence of jamming signals emitted by multi-antenna jammer on the covertness performance of the NOMA-based system. First, the detection performance of the warden is analyzed, and the optimal detection threshold and the MDEP of the warden are obtained. Then, with the aim of analyzing the covertness performance of the system, an optimization scheme is proposed, which maximizes the covert throughput by optimizing the PAF under the conditions of satisfying the covertness constraint and interruption constraint of the system. The key contributions of this work can be summarized as follows:

- We propose a scheme of covert communication which adopts a covert transmission strategy assisted by the multi-antenna jamming. The jamming adopts transmitting antenna selection (TAS) and random power with uniform distribution, which plays an uncertain role in the detection of the warden, so as to meet the requirements of covertness.
- We calculate the MDEP of the communication link between the transmitter and the covert user, obtain its closed-form expression which reveals the

effects of the transmitting power and the jamming power on MDEP, and deduce the range of its optimal detection threshold.
- The covert throughput is transformed into an optimization problem, which can maximize the covert throughput under the conditions of ensuring the covertness constraint and interruption constraint, so as to achieve a balance between the dependability and covertness of the communication system. By solving this problem, the optimal PAF is finally obtained.

1.2 Organization and Notations

The specific arrangements of each part are as follows. In Section II, the model and the jamming design of covert communication system based on NOMA are introduced. Section III first derives the detection error probability at Willie, and then discusses the optimal detection threshold and MDEP in the two cases. In Section IV, a scheme for optimizing the covertness of the system is provided. Section V presents the analysis of experimental numerical results, which verifies the correctness of theoretical analysis. The paper is summarized in Section VI.

Notations: $\mathcal{CN}\left(0,\sigma^2\right)$ is represented as a complex Gaussian random variable with a expectation of zero and a variance of σ^2. $\mathbb{E}\left(\cdot\right)$ denotes the expectation operation of random variables. Use $\left|\cdot\right|$ to represent the absolute value of a scalar. $\Pr\left(x\right)$ denotes the probability of a random variable x. In addition, $f_x\left(\cdot\right)$ and $F_x\left(\cdot\right)$ are the probability density function (PDF) and cumulative distribution function (CDF) of random variables, respectively. Finally, $\exp\left(\cdot\right)$ is the exponential function.

2 System Model

Firstly, the system model and the associated assumptions are introduced in detail. Secondly, with the aim of improving the system covertness, the jamming strategy is designed. Finally, the information transmission is described.

2.1 Model Introduction and Assumptions

As illustrated in Fig. 1, this paper considers the covert communication system based on NOMA. The system consists of a transmitter (Alice), a legal user (Bob), a warden (Willie), and a jammer (Carl). Among them, Alice intends to transmit two covert messages to Bob. In order for better spectrum utilization, NOMA technology is adopted. In this system, Willie is an eavesdropping user equipped with a power detector. Willie is passive and dumbly to observe the whole communication surrounding, trying to check whether Alice is sending private information to Bob. Willie uses a radiometer (power detector) to detect information transmission. If Willie detects a message passing,

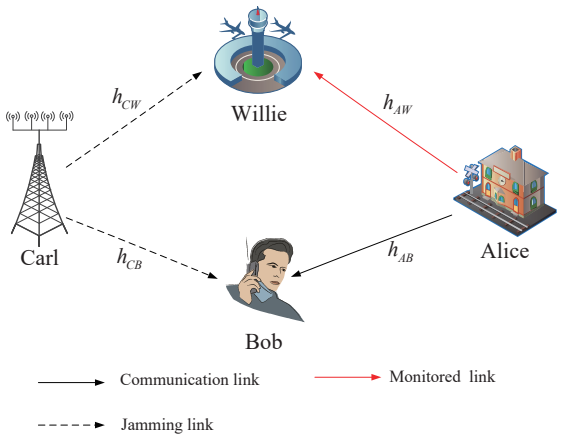

Fig. 1 System model based on NOMA.

it will cause some security risks to the communication link, such as location exposure, eavesdropping on messages, etc. Therefore, covertness becomes very important in the transmission of information. Carl is an auxiliary node in this environment. It is a jammer deployed by Alice or Bob and continuously sends artificial noise (AN). The purpose of arranging Carl in the system is to assist the covert communication and prevent Willie from detecting the covert information. In order to bring uncertainty to Willie's detection, Carl uses a random transmit power to interfere with the received signals of Willie.

Without lossing generality, the following assumptions are adopted in this paper: *i*) Alice, Bob and Willie are all configured with a single antenna, where Alice's antenna is used to send signals, while Bob and Willie's antennas are used to receive signals. Carl is configured with N_t antennas. h_{iB} and h_{iW} represent the channel fading coefficients from Carl's i-th ($i = 1, 2, ..., N_t$) antenna to Bob and Willie, respectively. *ii*) Carl and other nodes with one antenna work in half-duplex (HD) mode. *iii*) It is assumed that the CSI of Bob is available, while only statistical CSI of Willie is known. *iv*) The quasi-static Rayleigh fading channel is used as the wireless communication channel, that is, the channel coefficient remains unchanged in the same time slot, but the channel coefficient changes independently in different time slots. So all the wireless channels are independent of each other in the system. As shown in Fig. 1, the channel coefficients of the communication links between Alice and Bob, Alice and Willie, Carl and Bob, and Carl and Willie can be represented by $h_{AB} \sim \mathcal{CN}(0, \lambda_{AB})$, $h_{AW} \sim \mathcal{CN}(0, \lambda_{AW})$, $h_{iB} \sim \mathcal{CN}(0, \lambda_{CB})$, and $h_{iW} \sim \mathcal{CN}(0, \lambda_{CW})$, respectively.

2.2 Jamming Assist

In order to avoid Willie being able to correctly detect a NOMA-based covert transmission, Carl selects the transmit antenna to send the jamming signals

according to the optimal selection criteria, which is given by

$$i^* = \underset{1 \le i \le N_t}{\arg\min} R_{iB}, \tag{1}$$

where R_{iB} represents the signal-to-interference-plus-noise rate (SINR) from Carl's i-th antenna to Bob.

In the communication system, Willie only has the statistical CSI of h_{AW} and h_{CW} at each slot. If the jamming power P_C sent by Carl remains a fixed constant, Willie can learn the value of the jamming power over many observations and then remove it as background noise. Once Alice sends a covert message to Bob, Willie can directly detect the covert information. The purpose of introducing random transmitting power at Carl is to provide uncertainty in the received powers of Willie. Therefore, when the received power increases, Willie will not know whether Alice is sending private information to Bob or a change in the jamming power of Carl. P_C varies randomly between each time slot. We choose a continuous uniform distribution in $[0, P_C^{\max}]$ whose PDF is shown by

$$f_{P_C}(x) = \begin{cases} \dfrac{1}{P_C^{\max}}, 0 \le x \le P_C^{\max} \\ 0 \end{cases}, \tag{2}$$

where $P_C^{\max}$ is the maximum transmitting power of Carl. Willie is only familiar with the distribution of P_C, but is not aware of the instantaneous value, which helps to realize NOMA-based covert communication.

2.3 Information Transmission

Alice transmits the superimposed covert information to Bob, which is expressed as

$$\mathbf{x} = \sqrt{\varphi P_A}\mathbf{x}_1 + \sqrt{(1-\varphi)P_A}\mathbf{x}_2, \tag{3}$$

where P_A represents the transmitting power of Alice, which satisfies $0 < P_A \le P_A^{\max}$. $\mathbf{x}_1 \in \mathbb{C}^{1\times N}$ and $\mathbf{x}_2 \in \mathbb{C}^{1\times N}$ represent the two covert information sent by Alice, and satisfy $\mathbb{E}\left(|x_1[n]|^2\right) = \mathbb{E}\left(|x_2[n]|^2\right) = 1$, given $n \in \{1, 2, \ldots N\}$. φ is the power allocation factor (PAF) that determines the amount of transmitting power which Alice allocates to the two covert messages. We assume the priority of the two covert messages, where the higher priority is $\mathbf{x}_1$. More transmitting power will be allocated to $\mathbf{x}_1$, so $0.5 < \varphi \le 1$. When Alice does not send the superposition signal, the received signal $\mathbf{y}_B^0 \in \mathbb{C}^{1\times N}$ at Bob is expressed as

$$\mathbf{y}_B^0 = \sqrt{P_C}h_{i^*B}\mathbf{x}_C + \mathbf{n}_B, \tag{4}$$

where $\mathbf{x}_C \in \mathbb{C}^{1\times N}$ represents the jamming signal sent by Carl. h_{i^*B} is the channel coefficient from the optimal antenna selected by Carl through TAS

to Bob. P_C denotes the transmitting power of Carl. $\mathbf{n}_B \in \mathbb{C}^{1\times N}$ denotes the AWGN at Bob, and $\mathbf{n}_B$ obeys the cyclically symmetric complex Gaussian distribution with the expectation of 0 and the standard variance of σ_B^2. When Alice sends the superimposed covert signal, the signal $\mathbf{y}_B^1 \in \mathbb{C}^{1\times N}$ received at Bob is represented as

$$\mathbf{y}_B^1 = h_{AB}\left(\sqrt{\varphi P_A}\mathbf{x}_1 + \sqrt{(1-\varphi)\,P_A}\mathbf{x}_2\right) + \sqrt{P_C}h_{i^*B}\mathbf{x}_C + \mathbf{n}_B. \tag{5}$$

3 DETECTION INDICATORS AT WILLIE

In this section, we analysis the detection performance of Willie in detail. Firstly, Willie uses a power detector to perform binary detection on the received power. Secondly, the detection error probability of Willie is calculated. Willie's optimal detection threshold is solved analytically in the end.

3.1 Received Signal at Willie

For one communication slot, Willie is supposed to make a judgment on the following two assumptions in order to detect whether Alice is sending private information to Bob. There are two possibilities for receiving the signal at Willie. The corresponding received signal $\mathbf{y}_W \in \mathbb{C}^{1\times N}$ is given by

$$\mathbf{y}_W = \begin{cases} \sqrt{P_C}h_{i^*W}\mathbf{x}_C + \mathbf{n}_W, & H_0 \\ h_{AW}\left(\sqrt{\varphi P_A}\mathbf{x}_1 + \sqrt{(1-\varphi)\,P_A}\mathbf{x}_2\right) + \sqrt{P_C}h_{i^*W}\mathbf{x}_C + \mathbf{n}_W, & H_1 \end{cases}, \tag{6}$$

where the null hypothesis H_0 represents the fact that covert signal is not sent in the communication network (non-covert transmission phase), while the alternative hypothesis H_1 represents the covert transmission phase (covert signal is being transmitted in the communication link). We observe that the value of P_C is constantly changing within a time slot, so the real-time value of P_C can not be learned by Willie.

Detecting whether $\mathbf{y}_W$ is from H_0 or H_1 is the ultimate goal of Willie. Using the Neyman-Pearson norm, we can obtain a determination criterion to minimize the detection error probability of Willie , which can be represented as

$$P_W \underset{D_0}{\overset{D_1}{\gtrless}} \tau, \tag{7}$$

where $P_W = \dfrac{1}{N}\|\mathbf{y}_W\|^2$ represents the average power received in one slot at Willie. τ is a judgment threshold determined by Willie in advance. D_0 and D_1 represent the judgment made by Willie that Alice did not send a superimposed

signal and Alice sent a superimposed signal to Bob, respectively. We take into account infinite transmission times in this system, that is, $N \to \infty$. Therefore, the average received power at Willie is expressed as

$$P_W = \begin{cases} P_C|h_{i^*W}|^2 + \sigma_W^2, & H_0 \\ P_A|h_{AW}|^2 + P_C|h_{i^*W}|^2 + \sigma_W^2, & H_1 \end{cases}, \tag{8}$$

where $\mathbf{n}_W \in \mathbb{C}^{1\times N}$ denotes the AWGN at Willie with expectation 0 and variance σ_W^2.

At the end of a certain time slot, Willie must make a judgment about the communication behavior of Alice based on his own observations. Due to the randomness of P_C, Willie may make a wrong judgment. If there is no communication behavior between Alice and Bob, the event of *false alarm* will occur when Willie determines that there is communication behavior between Alice and Bob. We use $P_{FA} = \Pr(D_1|H_0)$ to represent the false alarm probability. Similarly, if Alice sends a covert signal to Bob, a *miss detection* will occur when Willie determines that Alice does not send a covert signal to Bob. The probability of missed detection is represented by $P_{MD} = \Pr(D_0|H_1)$. In this system, it is assumed that H_0 and H_1 have the same prior probability, i.e., $\Pr(H_0) = \Pr(H_1) = 1/2$. Under this assumption, the detection error probability of Willie is used to measure its detection performance, which can be represented as

$$\xi = P_{FA} + P_{MD}. \tag{9}$$

There exists an arbitrarily small positive value ε. When $\xi \geq 1-\varepsilon$ is true, it is considered that covert communication between Alice and Bob can be realized. Therefore, $\xi \geq 1-\varepsilon$ is called the covertness constraint. Next, we derive the P_{FA} and P_{MD}, and get their closed expressions.

3.2 Detection Error Probability

The P_{FA} and P_{MD} can be expressed as

$$P_{FA} = \begin{cases} 1, & \tau < \sigma_W^2 \\ 1 - \dfrac{\tau - \sigma_W^2}{P_C^{\max}|h_{i^*W}|^2}, & \sigma_W^2 \leq \tau < \rho_1 + \sigma_W^2 \\ 0, & \tau \geq \rho_1 + \sigma_W^2 \end{cases}, \tag{10}$$

and

$$P_{MD} = \begin{cases} 0, & \tau < \rho_2 + \sigma_W^2 \\ \dfrac{\tau - \rho_2 - \sigma_W^2}{P_C^{\max}|h_{i^*W}|^2}, & \rho_2 + \sigma_W^2 \leq \tau < \rho_3 + \sigma_W^2 \\ 1, & \tau \geq \rho_3 + \sigma_W^2 \end{cases}, \tag{11}$$

respectively, where $\rho_1 = P_C^{\max}|h_{i^*W}|^2$, $\rho_2 = P_A|h_{AW}|^2$, $\rho_3 = P_C^{\max}|h_{i^*W}|^2 + P_A|h_{AW}|^2$.

Proof : See Appendix A.

Theorem 1 *The detection error probability of Willie can be denoted as When* $\rho_1 \leq \rho_2$,

$$\xi = \begin{cases} 1, & \tau < \sigma_W^2 \\ 1 - \dfrac{\tau - \sigma_W^2}{P_C^{\max}|h_{i^*W}|^2}, & \sigma_W^2 \leq \tau < \rho_1 + \sigma_W^2 \\ 0, & \rho_1 + \sigma_W^2 \leq \tau < \rho_2 + \sigma_W^2 \\ \dfrac{\tau - \rho_2 - \sigma_W^2}{P_C^{\max}|h_{i^*W}|^2}, & \rho_2 + \sigma_W^2 \leq \tau < \rho_3 + \sigma_W^2 \\ 1, & \tau \geq \rho_3 + \sigma_W^2 \end{cases}, \tag{12}$$

and when $\rho_1 > \rho_2$,

$$\xi = \begin{cases} 1, & \tau < \sigma_W^2 \\ 1 - \dfrac{\tau - \sigma_W^2}{P_C^{\max}|h_{i^*W}|^2}, & \sigma_W^2 \leq \tau < \rho_2 + \sigma_W^2 \\ 1 - \dfrac{\rho_2}{P_C^{\max}|h_{i^*W}|^2}, & \rho_2 + \sigma_W^2 \leq \tau < \rho_1 + \sigma_W^2 \\ \dfrac{\tau - \rho_2 - \sigma_W^2}{P_C^{\max}|h_{i^*W}|^2}, & \rho_1 + \sigma_W^2 \leq \tau < \rho_3 + \sigma_W^2 \\ 1, & \tau \geq \rho_3 + \sigma_W^2 \end{cases}. \tag{13}$$

Proof : We find that there are several key values for the independent variable τ. These values are σ_W^2, ρ_1, ρ_2 and ρ_3. It is obvious that ρ_1, ρ_2 and ρ_3 are both greater than σ_W^2, while ρ_1 and ρ_2 are both less than ρ_3. The value of ρ_1 and ρ_2 varies with the change of $|h_{i^*W}|^2$ and $|h_{AW}|^2$ in different time slots. Therefore, comparing the sizes of ρ_1 and ρ_2, the corresponding detection error probability can be obtained by Eq. (9).

3.3 Optimal Detection Threshold

From the Willie's point of view, the goal is to minimize the performance of the covert system by choosing the appropriate threshold. We define the optimal detection threshold τ^* as the threshold that minimizes detection error probability of the system.

Theorem 2 *Willie detects the signal through the power detector, and the optimal detection threshold can be obtained as*

$$\tau^* = \begin{cases} \left[\rho_1 + \sigma_W^2, \rho_2 + \sigma_W^2\right], \rho_1 \leq \rho_2 \\ \left[\rho_2 + \sigma_W^2, \rho_1 + \sigma_W^2\right], \rho_1 > \rho_2 \end{cases}. \tag{14}$$

The corresponding minimum detection error probability (MDEP) is denoted by

$$\xi^* = \begin{cases} 0, & \rho_1 \le \rho_2 \\ 1 - \dfrac{P_A|h_{AW}|^2}{P_C^{\max}|h_{i^*W}|^2}, & \rho_1 > \rho_2 \end{cases}. \tag{15}$$

Proof : In order to minimize ξ, Willie tries to find an optimal threshold, which is allowed to be modeled as an optimization problem. This problem can be expressed as

$$\min_{\tau} \xi = P_{FA} + P_{MD}. \tag{16}$$

Case 1: $\rho_1 \le \rho_2$

It can be seen from Eq. (12) that $\xi = 1$ when $\tau < \sigma_W^2$ and $\tau \ge \rho_3 + \sigma_W^2$. This is a worst-case scenario for Willie. Therefore, τ^* is not set in this range by Willie. When $\sigma_W^2 \le \tau < \rho_1 + \sigma_W^2$, ξ decreases with the increase of τ. When $\rho_2 + \sigma_W^2 \le \tau < \rho_3 + \sigma_W^2$, ξ increases as the τ grows larger. When $\rho_1 + \sigma_W^2 \le \tau < \rho_2 + \sigma_W^2$, $\xi \triangleq 0$ remains unchanged. Analyzing the monotonicity of ξ with respect to τ, we can clearly see that $\xi = 0$ is best case for Willie when $\rho_1 + \sigma_W^2 \le \tau < \rho_2 + \sigma_W^2$. Therefore, Willie sets τ^* in this range. In this case, covert communication is 100% detected.

Case 2: $\rho_1 > \rho_2$

It can be seen from Eq. (13) that $\xi = 1$ when $\tau < \sigma_W^2$ and $\tau \ge \rho_3 + \sigma_W^2$. Similar to *Case 1*, Willie's detection performance is the worst at this time. When $\sigma_W^2 \le \tau < \rho_2 + \sigma_W^2$, ξ decreases monotonically with respect to τ and when $\rho_1 + \sigma_W^2 \le \tau < \rho_3 + \sigma_W^2$, ξ increases monotonically with respect to τ. When $\rho_2 + \sigma_W^2 \le \tau < \rho_1 + \sigma_W^2$, $\xi = 1 - \rho_2 \Big/ \left(P_C^{\max}|h_{i^*W}|^2\right)$ is a constant. Through the analysis of the monotonicity of ξ with respect to τ, it can be found that the detection error probability $\xi = 1 - \rho_2 \Big/ \left(P_C^{\max}|h_{i^*W}|^2\right)$ is the smallest when $\rho_2 + \sigma_W^2 \le \tau < \rho_1 + \sigma_W^2$, so τ^* is set in this interval.

These two cases can prove **Theorem 2**. It is worth noting that σ_W^2 only has an effect on τ^* and no effect on ξ^* when $\rho_1 > \rho_2$ in Eq. (14) and (15). This indicates that Willie has learned the noise power through long-term observation. If P_C is fixed, Willie can also obtain its value through observation. Therefore, uniform distribution is introduced at P_C. Moreover, the limit value of jamming power also directly affects the MDEP of Willie. When $P_C^{\max} \to \infty$, $\xi^* \to 1$, that is, covert communication is not detected.

4 The Optimization Of Covertness Performance

In this section, the covert communication is firstly designed from the aspect of the covert user Bob. Secondly, the covert throughput is maximized by optimizing the PAF in conditions of covertness constraint and reliability constraint.

4.1 Average MDEP

Since Willie is only known for its statistical CSI, we evaluate the covertness performance of system by getting the expectation of ξ^* about h_{AW} and h_{i^*W}, and select $\bar{\xi^*} \geq 1-\varepsilon$ as the feasible constraint of covert communication.

Theorem 3 *Under the optimal detection threshold, the average MDEP of Wiliie can be expressed as*

$$\bar{\xi^*} = \mathbb{E}\left(\xi^*\right) = \varpi - \frac{1}{2}\left[\varpi^2\left(1-\varpi\right)\right] F\left(1,2;3;\varpi\right), \tag{17}$$

where $\varpi = \dfrac{\lambda_{CW} P_C^{\max}}{\lambda_{AW} P_A + \lambda_{CW} P_C^{\max}}$, $F\left(a,b;c;d\right)$ *is the hypergeometric distribution.*

Proof : See Appendix B.

4.2 Outage Probability

The receiver Bob decodes the received signals on account of the SIC of NOMA. Since the $\mathbf{x}_1$ is assumed to possess a higher priority in this paper, the more power will be assigned to it, namely $0.5 < \varphi \leq 1$. When decoding superimposed signal, Bob firstly decodes $\mathbf{x}_1$ and considers $\mathbf{x}_2$ as jamming, then removes $\mathbf{x}_1$ from the superimposed signal through SIC, and finally decodes $\mathbf{x}_2$. According to Eq. (5), the SINR of $\mathbf{x}_1$ decoded at Bob is given by

$$\gamma_1 = \frac{\left|h_{AB}\right|^2 \varphi P_A}{\left|h_{AB}\right|^2 \left(1-\varphi\right) P_A + \left|h_{i^*B}\right|^2 P_C + \sigma_B^2}. \tag{18}$$

After SIC, the SINR of $\mathbf{x}_2$ is expressed as

$$\gamma_2 = \frac{\left|h_{AB}\right|^2 \left(1-\varphi\right) P_A}{\left|h_{i^*B}\right|^2 P_C + \sigma_B^2}, \tag{19}$$

where the CDF of $\left|h_{i^*B}\right|^2$ is denoted as

$$F_{\left|h_{i^*B}\right|^2}\left(x\right) = 1 - \exp\left(-\frac{N_t}{\lambda_{CB}} x\right). \tag{20}$$

$\mathbb{C}_1 = \log\left(\gamma_1 + 1\right)$ and $\mathbb{C}_2 = \log\left(\gamma_2 + 1\right)$ are the corresponding channel capacities.

Due to the uncertainty of h_{AB}, h_{i^*B} and P_C and the imperfection of SIC, Bob may not be able to decode $\mathbf{x}_1$ and $\mathbf{x}_2$. Therefore, in order to measure the reliability of this system, we derive the OP.

Theorem 4 *When decoding the instructions* $\mathbf{x}_1$ *and* $\mathbf{x}_2$ *at Bob, the corresponding OP can be expressed as*

$$P_1 = 1 - \frac{N_t \lambda_{AB}}{P_C^{\max} \lambda_{CB} \lambda_I} e^{-\frac{\lambda_I \sigma_B^2}{\lambda_{AB}}} \ln\left(1 + \frac{\lambda_{CB} \lambda_I P_C^{\max}}{N_t \lambda_{AB}}\right), \tag{21}$$

and

$$P_2 = 1 - \frac{N_t \lambda_{AB}}{P_C^{\max} \lambda_{CB} \lambda_{II}} e^{-\frac{\lambda_{II} \sigma_B^2}{\lambda_{AB}}} \ln\left(1 + \frac{\lambda_{CB} \lambda_{II} P_C^{\max}}{N_t \lambda_{AB}}\right), \tag{22}$$

respectively. Where $\mu_1 = 2^{R_1} - 1$, $\mu_2 = 2^{R_2} - 1$, $\lambda_I = \mu_1/(\varphi P_A - (1-\varphi) P_A \pi_1)$ *and* $\lambda_{II} = \mu_2/((1-\varphi) P_A)$. R_1 *and* R_2 *are the preset target rates of* $\mathbf{x}_1$ *and* $\mathbf{x}_2$*, respectively.*

Proof : See Appendix C.

4.3 Maximize Covert Throughput

In this section, since the instruction $\mathbf{x}_1$ is assumed to have a higher priority, we choose to optimize the performance of $\mathbf{x}_1$ while ensuring the reliability of $\mathbf{x}_2$. Covert throughput is the number of covert information successfully transmitted per unit time, which can measure the effectiveness of legitimate communication links. Therefore, the covert throughput is adopted as the standard to measure $\mathbf{x}_1$, which is defined as $\Gamma_1 = (1 - P_1) R_1$. For the covert communication system, an optimization scheme is given, which maximizes the covert throughput.

The problem of maximizing the covert throughput Γ_1 by optimizing the PFA φ under the given covertness constraint and reliability constraint can be expressed as

$$\begin{aligned} &\max_{\varphi, P_A} \Gamma_1 = (1 - P_1) R_1 \\ &s.t. \quad \bar{\xi}^* \geq 1 - \varepsilon \\ &\qquad P_2 \leq P_{th} \end{aligned}, \tag{23}$$

where P_{th} is the maximum OP allowed by the instruction $\mathbf{x}_2$.

The optimization problem is solved in three steps. Firstly, when Carl's maximum jamming power $P_C^{\max}$ remains unchanged and the covertness constraint in Eq. (23) is satisfied, the maximum value of P_A is calculated and denoted as P_A^*. Then, the maximum φ is obtained by the Lagrange function, which is denoted as φ^*. The Lagrange function is solved by Karsh-Kuhn-Tucker (KKT) condition, which is expressed as

$$\mathcal{L}(\varphi, \alpha, \beta) = (1 - P_1) R_1 + \alpha \left[\bar{\xi}^* - (1 - \varepsilon)\right] + \beta (P_{th} - P_2), \tag{24}$$

where α and β are both Lagrange multipliers. Finally, φ^* satisfying Eq. (24) is substituted into $\Gamma_1 = (1 - P_1) R_1$ to acquire the maximum covert throughput of $\mathbf{x}_1$.

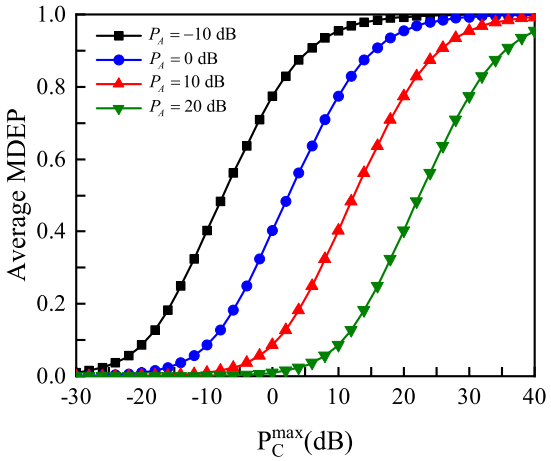

Fig. 2 Average MDEP versus $P_C^{\max}$ for different values of P_A.

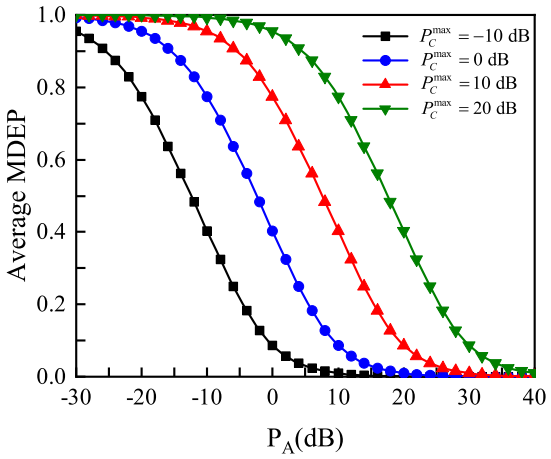

Fig. 3 Average MDEP versus P_A for different $P_C^{\max}$.

5 Numerical Analysis

In this section, the theoretical analysis obtained from the simulation directly verifies the correctness of the conclusions in Section III and IV. We analyze and investigate this system performance in different system parameters. For simplicity, the channel parameters are set as $\lambda_{AB} = \lambda_{AW} = \lambda_{CB} = \lambda_{CW} = 1$, the antenna number at Carl is set to $N_t = 3$, and the noise variance of Bob is $\sigma_B^2 = 1$ dB.

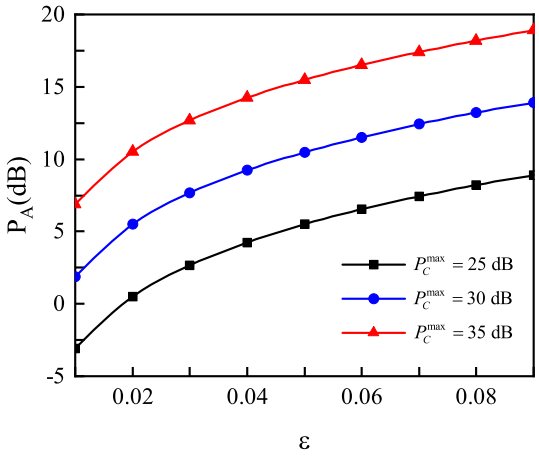

Fig. 4 P_A versus ε for different values of $P_C^{\max}$.

Fig. 2 shows the variation curves of the average MDEP $\bar{\xi}^*$ and $P_C^{\max}$ for different P_A. It is clear that the average MDEP $\bar{\xi}^*$ of Willie increases as the $P_C^{\max}$ grows larger. $P_C^{\max}$ is the maximum jamming power of Carl, and the larger $P_C^{\max}$ will make the increase of Willie's received power more uncertain. When detecting the received power of Willie, it is not known whether the increase in power is due to the covert message sent by Alice or the jamming signal sent by Carl. Therefore, when $P_C^{\max}$ is large enough, the average MDEP $\bar{\xi}^*$ gradually approaches 1, i.e. $\bar{\xi}^* \to 1$. This means it will be difficult for Willie to detect covert communication. In addition, the transmit power P_A of Alice also directly affects $\bar{\xi}^*$. Given $P_C^{\max}$, as P_A increases, $\bar{\xi}^*$ gradually decreases.

Fig. 3 depicts the relationship between average MDEP $\bar{\xi}^*$ and transmission power P_A for different $P_C^{\max}$. From Fig. 3, we can observe that the average MDEP $\bar{\xi}^*$ decreases as P_A increases. This indicates that if Alice uses a higher transmitting power to transmit covert messages, there is a larger probability of being detected by Willie. Therefore, when P_A is large enough, $\bar{\xi}^* \to 0$.

In Fig. 4, we draw the transmitting power P_A of Alice versus the covertness constraint ε for different $P_C^{\max}$. A phenomenon can be clearly obtained that P_A increases with the increase of ε. This means that larger ε will lead to a smaller demand for covertness, so P_A is correspondingly increased to meet the smaller demand for covertness. In addition, we can improve P_A by increasing $P_C^{\max}$, so as to better the covertness of the communication system. Therefore, in order to make Alice have a high transmitting power P_A, we should set $P_C^{\max}$ as large as possible.

Fig. 5 shows the curves of the optimal PAF φ^* and covertness constraint ε with $P_C^{\max} = 30$ dB, 35 dB, and $P_{th} = 0.4$, 0.45. It can be noticed that φ^* gradually increases as the ε rises, that is, more P_A will be allocated to $\mathbf{x}_1$ as the increase of ε under a certain condition of P_{th} and $P_C^{\max}$. With the gradual

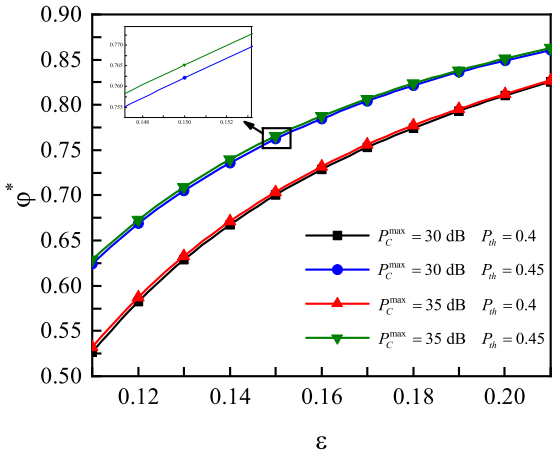

Fig. 5 φ^* for different $P_C^{\max}$ and P_{th} vs. ε.

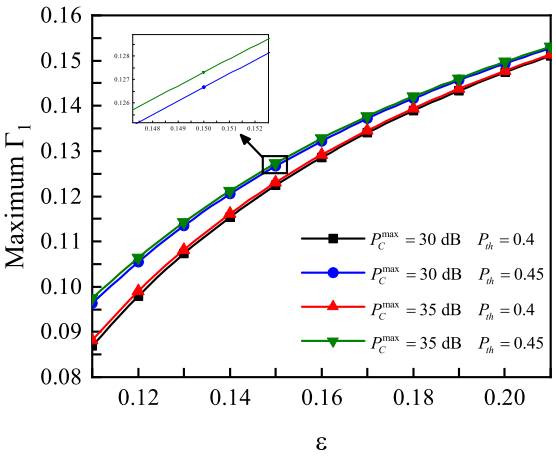

Fig. 6 Maximum Γ_1 for different $P_C^{\max}$ and P_{th} vs. ε.

increase of ε, the covertness requirement of the system will decrease. Therefore, there will be more power to help the covert messages to be transferred. In addition, when ε and $P_C^{\max}$ are constants, the larger the P_{th}, the smaller the reliability requirement of $\mathbf{x}_2$, so more power will be allocated to $\mathbf{x}_1$. As ε and P_{th} remain constants, $P_C^{\max}$ has almost no effect on φ^*.

Fig. 6 demonstrates the relationship between maximum covert throughput Γ_1 and covertness constraint ε for different $P_C^{\max}$ and P_{th}. As the figure shows, Γ_1 is a monotonically increasing function with respect to ε. It is also observed that Γ_1 increases with the increase of $P_C^{\max}$ and P_{th} when ε remains a fixed

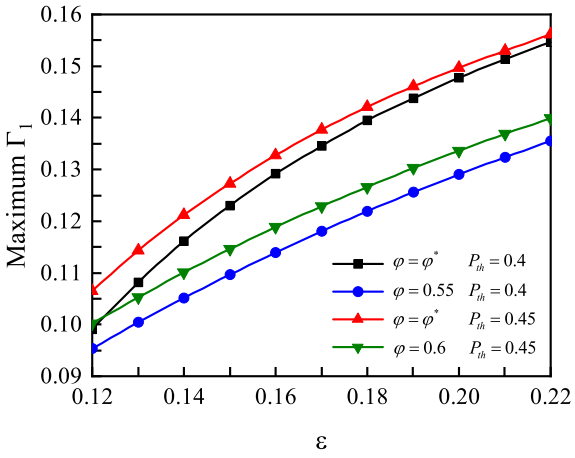

Fig. 7 Maximum Γ_1 vs. ε with different φ and P_{th}.

constant. This phenomenon indicates that increasing by $P_C^{\max}$ and P_{th} will increase the power allocated to $\mathbf{x}_1$, thereby increasing the covert throughput. Meanwhile, it can be observed that P_{th} compared with $P_C^{\max}$ has a greater impact on Γ_1.

In Fig. 7, we compare the maximum covert throughput Γ_1 versus covertness constraint ε when the PAF φ is taken at the optimal and non-optimal values (e.g., $\varphi = 0.55, 0.6$) for different P_{th}. One can observe that Γ_1 at the optimal value of φ is significantly greater than Γ_1 at the non-optimal value of φ under the same interruption constraint, which fully demonstrates that the proposed optimization scheme does improve the covertness performance of system.

6 Conclusion

In this paper, a covert communication assisted by multi-antenna jamming scheme based on NOMA is proposed. Specifically, the multi-antenna jammer Carl transmits a random jamming signal to provide cover for the communication between the transmitter Alice and the legitimate user Bob. Based on the proposed scheme, the optimal detection threshold and its corresponding average MDEP are derived. With the aim of balancing the reliability and covertness of this system, we propose an optimization strategy to maximize the covert throughput and obtain the optimal solution. Finally, these analysis results illustrate that the covertness performance of this system can be improved by the proposed scheme to a certain extent. In future work, we consider extending the single user to multiple users for covert communication.

APPENDIX A

According to Eq. (8), the false alarm probability P_{FA} can be denoted by

$$\begin{aligned} P_{FA} &= \Pr\left(D_1 \left| H_0 \right.\right) = \Pr\left(P_W > \tau \left| H_0 \right.\right) \\ &= \Pr\left(P_C |h_{i^*W}|^2 + \sigma_W^2 > \tau\right) \\ &= \begin{cases} 1, & \tau < \sigma_W^2 \\ \int_{\frac{\tau-\sigma_W^2}{|h_{i^*W}|^2}}^{P_C^{\max}} f_{P_C}(x), & \sigma_W^2 \le \tau < \rho_1 + \sigma_W^2 \\ 0, & \tau \ge \rho_1 + \sigma_W^2 \end{cases} . \end{aligned} \tag{A.1}$$

Similarly, the miss detection probability P_{MD} can be denoted by

$$\begin{aligned} P_{MD} &= \Pr\left(D_0 \left| H_1 \right.\right) = \Pr\left(P_W \le \tau \left| H_1 \right.\right) \\ &= \Pr\left(P_A |h_{AW}|^2 + P_C |h_{i^*W}|^2 + \sigma_W^2 \le \tau\right) \\ &= \begin{cases} 0, & \tau < \rho_2 + \sigma_W^2 \\ \int_0^{\frac{\tau-\rho_2-\sigma_W^2}{|h_{i^*W}|^2}} f_{P_C}(x), & \rho_2 + \sigma_W^2 \le \tau < \rho_3 + \sigma_W^2 \\ 1, & \tau \ge \rho_3 + \sigma_W^2 \end{cases} , \end{aligned} \tag{A.2}$$

where the PDF of jamming power P_C can be seen from Eq. (2).

The results of Eq. (10) and (11) can be obtained through Eq. (A.1) and (A.2).

APPENDIX B

According to Eq. (15), the average MDEP can be denoted as

$$\mathbb{E}\left(\xi^*\right) = \Pr\left(\rho_1 \le \rho_2\right) \mathbb{E}\left(\xi^* \left| \rho_1 \le \rho_2 \right.\right) + \Pr\left(\rho_1 > \rho_2\right) \mathbb{E}\left(\xi^* \left| \rho_1 > \rho_2 \right.\right), \tag{B.1}$$

Since $\mathbb{E}\left(\xi^* \left| \rho_1 \le \rho_2 \right.\right)$ is 0, we just have to solve for $\Pr\left(\rho_1 > \rho_2\right)$ and $\mathbb{E}\left(\xi^* \left| \rho_1 > \rho_2 \right.\right)$ to get $\mathbb{E}\left(\xi^*\right)$.

Next, $\Pr\left(\rho_1 > \rho_2\right)$ and $\mathbb{E}\left(\xi^* \left| \rho_1 > \rho_2 \right.\right)$ are solved in detail, which is expressed as

$$\begin{aligned} \Pr\left(\rho_1 > \rho_2\right) &= \Pr\left(P_C^{\max} |h_{i^*W}|^2 > P_A |h_{AW}|^2\right) \\ &= \int_0^{\infty} \int_0^{\frac{P_C^{\max} y}{P_A}} f_{|h_{AW}|^2}(x)\, f_{|h_{i^*W}|^2}(y) dx dy , \\ &= \frac{\lambda_{CW} P_C^{\max}}{\lambda_{AW} P_A + \lambda_{CW} P_C^{\max}} \end{aligned} \tag{B.2}$$

and

$$\begin{aligned}\mathbb{E}\left(\xi^{*}\left|\rho_{1}>\rho_{2}\right.\right) &= \mathbb{E}\left(1-\frac{P_{A}\left|h_{AW}\right|^{2}}{P_{C}^{\max}\left|h_{i^{*}W}\right|^{2}}\left|\rho_{1}>\rho_{2}\right.\right) \\ &= 1-\frac{P_{A}}{P_{C}^{\max}}\int_{0}^{\infty}\int_{0}^{\frac{P_{C}^{\max}y}{P_{A}}}\frac{x}{y}f_{|h_{AW}|^{2}}\left(x\right)f_{|h_{i^{*}W}|^{2}}\left(y\right)dxdy, \\ &= 1-\frac{P_{A}P_{C}^{\max}\lambda_{AW}\lambda_{CW}}{2(\lambda_{AW}P_{A}+\lambda_{CW}P_{C}^{\max})^{2}} \\ &\quad\times F\left(1,2;3;\frac{\lambda_{CW}P_{C}^{\max}}{\lambda_{CW}P_{C}^{\max}+\lambda_{AW}P_{A}}\right)\end{aligned} \tag{B.3}$$

respectively. Then substitute them into Eq. (B.1) to get the result of **Theorem 3**.

APPENDIX C

In the case of imperfect SIC, according to the definition of OP, it can be known that the outage event occurs at Bob when Bob cannot successfully decode $\mathbf{x}_1$, and the outage event also occurs when Bob fails to decode $\mathbf{x}_2$ after successfully decoding $\mathbf{x}_1$. Therefore, P_1 and P_2 are given as

$$\begin{aligned}P_{1} &= \Pr\left(\gamma_{1}<\mu_{1}\right) \\ &= \Pr\left(|h_{AB}|^{2}<\frac{\mu_{1}|h_{i^{*}B}|^{2}P_{C}+\mu_{1}\sigma_{B}^{2}}{\varphi P_{A}-\mu_{1}\left(1-\varphi\right)P_{A}}\right) \\ &= \int_{0}^{P_{C}^{\max}}\int_{0}^{\infty}\int_{0}^{\lambda_{I}\left(yz+\sigma_{B}^{2}\right)}\frac{N_{t}}{P_{C}^{\max}\lambda_{AB}\lambda_{CB}}e^{-\frac{\lambda_{CB}x+N_{t}\lambda_{AB}y}{\lambda_{AB}\lambda_{CB}}}dxdydz\end{aligned}, \tag{C.1}$$

and

$$\begin{aligned}P_{2} &= P_{1}+\Pr\left(\gamma_{2}<\mu_{2},\gamma_{1}\geq\mu_{1}\right) \\ &= P_{1}+\Pr\left(\frac{\mu_{1}|h_{i^{*}B}|^{2}P_{C}+\mu_{1}\sigma_{B}^{2}}{\varphi P_{A}-\mu_{1}\left(1-\varphi\right)P_{A}}\leq|h_{AB}|^{2}<\frac{\mu_{2}|h_{i^{*}B}|^{2}P_{C}+\mu_{2}\sigma_{B}^{2}}{\left(1-\varphi\right)P_{A}}\right), \\ &= P_{1}+\int_{0}^{P_{C}^{\max}}\int_{0}^{\infty}\int_{\lambda_{I}\left(yz+\sigma_{B}^{2}\right)}^{\lambda_{II}\left(yz+\sigma_{B}^{2}\right)}\frac{N_{t}}{P_{C}^{\max}\lambda_{AB}\lambda_{CB}}e^{-\frac{\lambda_{CB}x+N_{t}\lambda_{AB}y}{\lambda_{AB}\lambda_{CB}}}dxdydz\end{aligned} \tag{C.2}$$

respectively.

Acknowledgment

This work was supported by the Key Research Project of Henan Higher Education Institution (Grant No. 17B440001), Henan University of Science and

Technology Enterprise Commissioning Project (Grant No. JG017), and Henan Provincial Science and Technology Tackling Program (Grant No. 212102210504, No. 212102210557).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Y. Tao, L. Liu, S. Liu, and Z. Zhang, "A survey: Several technologies of non-orthogonal transmission for 5G," *China Communications*, vol. 12, no. 10, pp. 1–15, Oct. 2015.
2. L. P. Qian, B. Shi, Y. Wu, B. Sun, and D. H. K. Tsang, "NOMA-enabled mobile edge computing for internet of things via joint communication and computation resource allocations," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 718–733, Jan. 2020.
3. Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.
4. Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, Feb. 2017.
5. Y. Wang, B. Ren, S. Sun, S. Kang, and X. Yue, "Analysis of non-orthogonal multiple access for 5G," *China Communications*, vol. 13, no. Supplement2, pp. 52–66, 2016.
6. X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, "Residual transceiver hardware impairments on cooperative NOMA networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 680–695, Jan. 2020.
7. Y. Liu, H. Xing, C. Pan, A. Nallanathan, M. Elkashlan, and L. Hanzo, "Multiple-antenna-assisted non-orthogonal multiple access," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 17–23, Apr. 2018.
8. W. Peng, W. Gao, and J. Liu, "A novel perspective on multiple access in 5G network: Framework and solutions," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 154–160, Jun. 2019.
9. L. Zhang, M. Xiao, G. Wu, M. Alam, Y.-C. Liang, and S. Li, "A survey of advanced techniques for spectrum sharing in 5G networks," *IEEE Wireless Communications*, vol. 24, no. 5, pp. 44–51, Oct. 2017.
10. X. Li, Y. Zheng, M. D. Alshehri, L. Hai, V. Balasubramanian, M. Zeng, and G. Nie, "Cognitive AmBC-NOMA IoV-MTS networks with IQI: Reliability and security analysis," *IEEE Transactions on Intelligent Transportation Systems*, 2021, doi: 10.1109/TITS.2021.3113995.
11. O. Shental, B. M. Zaidel, and S. S. Shitz, "Low-density code-domain NOMA: Better be regular," in *2017 IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2628–2632.
12. S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-s. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 721–742, Second quarter, 2017.
13. D. Wan, M. Wen, F. Ji, H. Yu, and F. Chen, "Non-orthogonal multiple access for cooperative communications: Challenges, opportunities, and trends," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 109–117, Apr. 2018.
14. Y. N. Ahmed, "A novel scheduling technique for NOMA in 5G wireless communication systems," in *2019 12th German Microwave Conference (GeMiC)*, Stuttgart, Germany, Mar. 2019, pp. 59–62.

15. J. Ju, W. Duan, Q. Sun, S. Gao, and G. Zhang, "Performance analysis for cooperative NOMA with opportunistic relay selection," *IEEE Access*, vol. 7, pp. 131 488–131 500, 2019.
16. X. Li, M. Zhao, M. Zeng, S. Mumtaz, V. G. Menon, Z. Ding, and O. A. Dobre, "Hardware impaired ambient backscatter NOMA systems: Reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, Apr. 2021.
17. W. U. Khan, X. Li, A. Ihsan, M. A. Khan, V. G. Menon, and M. Ahmed, "NOMA-enabled optimization framework for next-generation small-cell IoV networks under imperfect SIC decoding," *IEEE Transactions on Intelligent Transportation Systems*, 2021, doi: 10.1109/TITS.2021.3091402.
18. R. Huang, D. Wan, F. Ji, H. Qing, J. Li, H. Yu, and F. Chen, "Performance analysis of NOMA-based cooperative networks with relay selection," *China Communications*, vol. 17, no. 11, pp. 111–119, Nov. 2020.
19. Y. Li, Y. Li, X. Chu, Y. Ye, and H. Zhang, "Performance analysis of relay selection in cooperative NOMA networks," *IEEE Communications Letters*, vol. 23, no. 4, pp. 760–763, Apr. 2019.
20. C. Guo, J. Xin, L. Zhao, and X. Chu, "Performance analysis of cooperative NOMA with energy harvesting in multi-cell networks," *China Communications*, vol. 16, no. 11, pp. 120–129, Nov. 2019.
21. X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu, and A. Nallanathan, "Secure communications in a unified non-orthogonal multiple access framework," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 2163–2178, Mar. 2020.
22. Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 4, pp. 938–953, Apr. 2016.
23. Y. Yin, Y. Peng, M. Liu, J. Yang, and G. Gui, "Dynamic user grouping-based NOMA over rayleigh fading channels," *IEEE Access*, vol. 7, pp. 110 964–110 971, 2019.
24. R. Oppliger, *Contemporary Cryptography, Second Edition.* Fitchburg, MA, USA: Artech House, 2011.
25. E. Sakk and S. P. Wang, "Code structures for quantum encryption and decryption," in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, Zhuhai, China, Jan. 2021, pp. 7–11.
26. Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, Apr. 2018.
27. J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, May. 2018.
28. B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.
29. Y. Chen, T. Zhang, Y. Liu, Y. Cai, W. Yang, and L. Wang, "Physical layer security in NOMA-enabled cognitive radio networks," in *IET 8th International Conference on Wireless, Mobile Multimedia Networks*, Beijing, China, Nov. 2019, pp. 43–48.
30. Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 700–714, Jun. 2019.
31. X. Li, H. Mengyan, Y. Liu, V. G. Menon, A. Paul, and Z. Ding, "I/Q imbalance aware nonlinear wireless-powered relaying of B5G networks: Security and reliability analysis," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2020.
32. Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
33. B. A. Bash, D. Goeckel, and D. Towsley, "Covert communication gains from adversarys ignorance of transmission time," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8394–8405, Dec. 2016.
34. O. A. Topal and G. K. Kurt, "Covert communication in cooperative NOMA networks," in *2020 28th Signal Processing and Communications Applications Conference (SIU)*, Gaziantep, Turkey, Oct. 2020, pp. 1–4.

35. Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in IoT systems: Hiding information in interference," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 46–52, Dec. 2018.
36. C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6313–6323, Apr. 2021.
37. O. Shmuel, A. Cohen, and O. Gurewitz, "Multi-antenna jamming in covert communication," *IEEE Transactions on Communications*, vol. 69, no. 7, pp. 4644–4658, Jul. 2021.
38. J. Hu, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert wireless communications with channel inversion power control in rayleigh fading," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12 135–12 149, Dec. 2019.
39. K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.
40. W. Xiong, Y. Yao, X. Fu, and S. Li, "Covert communication with cognitive jammer," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1753–1757, Oct. 2020.
41. K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–5.
42. S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 129–140, Jan. 2019.
43. M. Wang, W. Yang, Y. Wang, L. Tao, and R. Ma, "Covert communications in uplink NOMA systems with channel inversion power control," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, Chengdu, China, Dec. 2020, pp. 317–321.
44. Y. Jiang, L. Wang, H. Zhao, and H.-H. Chen, "Covert communications in D2D underlaying cellular networks with power domain NOMA," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3717–3728, Sep. 2020.
45. L. Tao, W. Yang, S. Yan, D. Wu, X. Guan, and D. Chen, "Covert communication in downlink NOMA systems with random transmit power," *IEEE Wireless Communications Letters*, vol. 9, no. 11, pp. 2000–2004, Nov. 2020.