Joint Covert and Secure Communication for SWIPT-Assisted CNOMA Systems

Gaojian Huang, *Member, IEEE*, Yuxin Lei, Xingwang Li, *Senior Member, IEEE*, Wali Ullah Khan, *Member, IEEE*, Gongpu Wang, *Senior Member, IEEE*, and Arumugam Nallanathan, *Fellow, IEEE*

***Abstract*—With the rapid advancement of physical-layer security technology, the covert and secure communication has become crucial in safeguarding wireless communication systems. In this article, we propose a joint covert and secure transmission scheme for simultaneous wireless information and power transfer (SWIPT) assisted cooperative nonorthogonal multiple access (CNOMA) systems. In the CNOMA system, a greedy relay transmits the confidential information to the far user (Carol), with the assistance of the near user (Bob). Meanwhile, as a SWIPT node, Bob is self-sustained by harvesting energy from relay. What is more, a warden (Alice) and noncolluding eavesdroppers (Eves) always attempt to detect and capture the confidential information, respectively. To counteract the attacks from Alice and Eves, a jamming-assisted scheme is employed. For the proposed system model, we derive closed-form expressions for the detection error probability (DEP) and the average minimum detection error probability (AMDEP) of Alice. Additionally, closed-form expressions for the outage probability (OP) of users and the intercept probability (IP) of Eves are obtained. Furthermore, to maximize the effective covert rate (ECR) of Carol, an optimization problem is formulated, subject to covertness and security constraints. Numerical results are provided to demonstrate the impact of the system parameters on covert and secure performance, with the results showing perfect agreement with the theoretical analysis.**

***Index Terms*—Cooperative nonorthogonal multiple access (CNOMA), covert communication, modify and forward (MF), physical-layer security (PLS), simultaneous wireless information and power transfer (SWIPT).**

I. Introduction

With the rapid development of wireless communication technologies, communication security has garnered significant attention. Physical-layer security (PLS), one of the most popular technologies in secure wireless communication, has been extensively investigated in recent years [1]. PLS leverages wireless channel characteristics to prevent private information from being decoded by eavesdroppers (Eve), and the concept of PLS was first introduced in [2], where it was demonstrated that nearly perfect secrecy could be achieved by exploiting the differences between the main channel and the wiretap channel. To improve the performance of PLS, various schemes have been proposed [3], [4], [5], [6], [7]. In [3], it considered a practical scenario where the transmitter does not have the channel state information (CSI) of eavesdroppers and showed that transmit antenna selection can positively affect PLS. A secure beamforming scheme for two-tier downlink heterogeneous networks was proposed in [4], and its effectiveness in improving secure performance was demonstrated through simulations. Additionally, in [5], it explored the benefits of artificial noise schemes in combating eavesdropping. In [6] and [7], uncoordinated cooperative jamming schemes were investigated to enhance security performance. Furthermore, a few studies have primarily focus on the security of NOMA systems, as exemplified by [8], [9], [10], [11], [12], and [13].

Beyond PLS, another secure communication technology, named covert communication, was introduced in [14]. Unlike PLS, covert communication aims to hide the existence of the confidential signal from the warden. To enhance covert communication, numerous efforts have been made in recent years [15], [16], [17], [18], [19], [20], [21], [22], [23], [24]. For instance, several studies improved covertness by exploiting various uncertainties, such as transmission time [15], CSI [16], [17], [18], [19], and artificial jamming [20], [21]. Additionally, technologies like simultaneously transmitting and

Received 8 January 2025; accepted 14 February 2025. Date of publication 19 February 2025; date of current version 9 June 2025. This work was supported in part by the China Postdoctoral Science Foundation under Grant 2024M750801; in part by the Key Scientific Research Projects of Higher Education Institutions in Henan Province under Grant 24A510004 and Grant 25A510003; in part by the Henan Scientific and Technological Research Project under Grant 242102210193 and Grant 252102211118; in part by the Henan Polytechnic University Fundamental Scientific Research Operating Expense Youth Exploration and Innovation Fund Project under Grant NSFRF230421; in part by the Surveying and Mapping Science and Technology Double First-Class Discipline Establishment Project for Nurturing High Level Research Topics under Grant GCCYJ202408; in part by the Fundamental Research Program of Shanxi Province under Grant 202303021211340; and in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2024D15. *(Corresponding author: Xingwang Li.)*

Gaojian Huang is with the School of Physics and Electronic Information Engineering, the School of Surveying and Land Information Engineering, and the Photoelectric Detection and Sensing Integrated Engineering Technology Research Center of Henan Province, Henan Polytechnic University, Jiaozuo 454003, China, and also with the Faculty of Data Science, City University of Macau, Macau, China (e-mail: g.huang@hpu.edu.cn).

Yuxin Lei is with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454003, China (e-mail: xin@home.hpu.edu.cn).

Xingwang Li is with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454099, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: lixingwangbupt@gmail.com).

Wali Ullah Khan is with the Interdisciplinary Center for Security, Reliability and Trust, University of Luxembourg, 1855 Luxembourg City, Luxembourg (e-mail: waliullah.khan@uni.lu).

Gongpu Wang is with the School of Computer Science and Technology, Beijing Jiaotong University, Beijing 100044, China (e-mail: gpwang@bjtu.edu.cn).

Arumugam Nallanathan is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, E1 4NS London, U.K., and also with the Department of Electronic Engineering, Kyung Hee University, Yongin 17104, South Korea (e-mail: a.nallanathan@qmul.ac.uk).

Digital Object Identifier 10.1109/JIOT.2025.3543573

reflecting reconfigurable intelligent surfaces (STAR-RIS) have been applied to assist covert communication [22], [23], [24]. In [22], a STAR-RIS covert communication system was investigated, showing that the effective covert rate (ECR) improves with an increased number of STAR-RIS elements. Covert communication systems have also been explored in diverse scenarios, such as device-to-device (D2D) underlaid cellular networks [23] and covert backscatter communication systems with powerful wardens [24]. These studies highlighted how antenna reflections and Gaussian signal variances negatively impact the warden's detection capabilities.

Most prior research focuses on scenarios with either warden(s) or eavesdropper(s). However, in certain contexts, particularly military operations, the coexistence of both warden(s) and eavesdropper(s) is likely. More recently, research has increasingly explored the joint covert and secure transmission, as summarized in [25], [26], [27], [28], [29], [30], [31], [32], [33], and [34]. Within this context, scenarios involving warden(s) and an untrusted relay were investigated in [25], [26], [27], and [28]. For instance, a two-phase covert and secure transmission strategy was proposed in [25], in which the jamming signal is sent to resist attacks from both a warden and an untrusted relay, and the instantaneous secrecy rate, subject to the covertness requirements, was maximized by using the proposed power allocation strategy. Building on this, in [26], it was extended the scenario to multiple wardens and untrusted relays. In [27], a covert and secure D2D network was proposed where a full-duplex base station emitted the jamming signal to assist communication. This study considered both underlay and overlay spectrum resource sharing modes, with corresponding optimization schemes proposed to maximize the average covert rate. In [28], to prevent the covert user's information from being detected by the warden and the secure user's information from being decoded by the untrusted user, the source transmitted the covert user's information in selected time slots, and the average rate, subject to both covertness and security requirements, was maximized. In contrast, studies in [29], [30], [31], [32], [33], and [34] investigated scenarios involving a warden and eavesdropper(s). In [29], a covert and secure communication system with artificial noise was studied, and low-complexity and analytical approaches were applied to maximize the secrecy rate, subject to covertness requirements. To resist attacks from both the warden and the eavesdropper, in [30], a communication scheme was proposed where the source sends the confidential signal in selected time slots, while a multiantenna cooperative jammer sends the jamming signal in all time slots. It was demonstrated that this system can achieve a certain level of covertness and security. Additionally, the use of reconfigurable intelligent surfaces (RIS) or STAR-RIS to enhance covertness and security has been explored in [31], [32], [33], and [34]. In [31], the source attempted to transmit covert information to one user and deliver secure information to another, with both a warden and an eavesdropper present. The optimization problem, aimed at maximizing the covert rate, was solved using a successive convex approximation method. In contrast to [31], in [32], a node that served as both a warden and an eavesdropper was considered, with RIS and rate-splitting (RS) technology applied to improve performance. This study showed that RS, NOMA, and RIS positively impact covertness. Furthermore, active RIS was explored in [33], where the system achieved a lower outage probability (OP) and a higher covert rate compared to passive RIS-based systems. In [34], a STAR-RIS-assisted multiantenna millimeter-wave joint covert and secure communication system was investigated. The simulation results reveal that STAR-RIS outperforms RIS in implementing both covert communication and physical-layer security (PLS) simultaneously.

While previous studies on joint covert and secure transmission focus on security, the issue of energy scarcity has been largely overlooked. Simultaneous wireless information and power transfer (SWIPT), a technology capable of decoding information and harvesting energy from the received signal, has the potential to significantly improve the energy efficiency of communication systems. Introduced in [35], SWIPT operates via two protocols: 1) time switching (TS) and 2) power splitting (PS). In TS, part of the time slot is used for energy harvesting (EH) and the rest for information transfer (IT). In PS, a portion of the received signal's power is used for EH, while the remainder is used for IT. On the other hand, NOMA technology has been widely investigated as a promising solution due to its ability to enhance user fairness and improve power efficiency [36], [37]. To further improve communication performance for weaker users in NOMA systems, Cooperative NOMA (CNOMA) was proposed in [38]. In CNOMA, stronger users acted as relays to assist communication between the source and weaker users which significantly improves the system's reliability and capacity [39], [40]. Inspired by this technology, SWIPT-assisted CNOMA systems have garnered significant interest in recent studies [41], [42], [43], [44], [45], [46]. In [41], a half-duplex hybrid SWIPT-assisted CNOMA system with transmit antenna selection scheme was explored, revealing that the block time for EH has a more substantial impact on the far user's communication performance than the PS ratio. In contrast, in [42], a SWIPT-assisted CNOMA system with a full-duplex multiple-antenna near user was considered, and a path-following algorithm, superior to conventional iterative methods, was proposed to maximize energy efficiency. In [43], a hybrid half-duplex (HD)/full-duplex (FD) SWIPT-assisted CNOMA system was studied, demonstrating superior performance compared to nonhybrid schemes. In [44], a multiple-user SWIPT-assisted CNOMA system was proposed, where near users with strong channels acted as relays for far users. In [45], a SWIPT-assisted CNOMA system with multiple base stations and near users assisting a far user was investigated. The simulation results showed significant performance improvements for the far user compared to conventional CNOMA and coordinated multipoint CNOMA schemes with opportunistic scheduling. In [46], a Poisson point process-distributed multitier SWIPT-assisted CNOMA system was proposed, where OP and throughput expressions were derived. It can be found that the recent studies on SWIPT-assisted CNOMA systems primarily focus on PLS. Furthermore, SWIPT-assisted CNOMA system has proven to be crucial in practical application scenarios, such as large-scale Internet of Things (IoT) systems [47], [48]

TABLE I
COMPARISON OF THE PREVIOUS WORKS AND OUR WORK (✓: CONSIDERED; ×: NOT CONSIDERED)

Ref./Prop.	NOMA /CNOMA	SWIPT	Jamming	Multiple Wardens /Eves	Covert Communication	PLS	Performance Metrics
[8]	✓	×	×	×	×	✓	SOP
[9]	✓	×	×	×	×	✓	OP, IP
[10]	✓	×	×	×	×	✓	Sum secrecy rate, Computational complexity
[11]	✓	×	×	×	×	✓	SOP
[12]	✓	×	×	×	×	✓	OP, IP, Throughput, Energy efficiency
[13]	✓	✓	×	✓	×	✓	SOP
[16]	✓	×	×	×	✓	×	DEP, AMDEP, OP, ECR
[18]	✓	×	✓	×	✓	×	DEP, COP, ECR
[22]	✓	×	×	×	✓	×	DEP, AMDEP, OP, ECR
[25]	×	×	✓	×	✓	✓	DEP, Ergodic secrecy rate
[26]	×	×	✓	✓	✓	✓	DEP, Ergodic secrecy rate
[27]	×	×	✓	×	✓	✓	DEP, AMDEP, OP, Average secrecy rate
[28]	✓	×	×	×	✓	✓	DEP, Covert rate, Secrecy rate
[29]	×	×	✓	✓	✓	✓	DEP, Secure rate, Average secrecy throughput
[30]	×	×	✓	✓	✓	✓	DEP, Ergodic secrecy rate
[31]	×	×	×	×	✓	✓	DEP, OP, Covert rate, Secrecy rate
[32]	✓	×	×	×	✓	✓	DEP, Covert rate, SOP
[33]	✓	×	×	×	✓	✓	DEP, OP, Covert rate, SOP
[34]	✓	×	×	×	✓	✓	DEP, Secure rate, Average sum rate
Our work	✓	✓	✓	✓	✓	✓	DEP, AMDEP, OP, IP, ECR

and autonomous aerial vehicle based disaster relief operations [49], [50].

A. Motivation and Contributions

Existing studies on joint covert and secure transmission often overlook the critical issue of energy scarcity. While some research has explored SWIPT-assisted CNOMA systems, these research typically employ simplistic and foundational models with limited emphasis on security performance. They all fall short of addressing the increasingly covertness and security requirements of modern communication systems. To bridge this gap, we propose a novel joint covert and secure transmission scheme for SWIPT-assisted CNOMA systems. Unlike the straightforward node cooperation strategies commonly adopted in previous research, our approach introduces a more complex cooperation model. Specifically, the source node transmits public signals, while the relay node performs multiple functions: forwarding public signals, transmitting confidential signal, and generating interference signal with random power to enhance both covertness and security. Our scheme considers a more challenging scenario in which obstacles prevent the relay node from directly transmitting the confidential signal to the far user. To overcome this limitation, the near user leverages EH technology to forward the confidential signal to the far user. Within this framework, each node is assigned a specific role and collaborates closely to mitigate threats from a monitoring source node and multiple noncolluding Eves. Building on this deep collaboration among multiple nodes, our work represents the first realization of joint covert and secure transmission in SWIPT-assisted CNOMA systems. This innovative approach holds significant theoretical value and practical application potential. To highlight the contributions of our work, Table I presents a comparative analysis of our proposed scheme and related studies. The contributions of this article can be summarized as follows.

1) To the best of our knowledge, this work is the first to investigate joint covert and secure transmission in a SWIPT-assisted CNOMA system. The proposed scheme has potential applications in large-scale IoT networks and autonomous aerial vehicle based disaster relief scenarios. In this work, we consider a communication scenario in a SWIPT-assisted CNOMA system involving a source (acting as a warden), a greedy relay, a far user, a near user, and multiple eavesdroppers. Given energy constraints, the near user serves as a SWIPT node to forward the confidential signal to the far user. The relay transmits a jamming signal with uncertain power to resist attacks from the warden and the eavesdroppers, enhancing both covertness and security.
2) The derived metrics provide a solid mathematical foundation for the theoretical analysis, allowing us to systematically examine the tradeoff between covertness and security. The optimization approach is beneficial to adjust the variables to satisfy different communication requirements, offering valuable insights for improving communication efficiency, particularly in resource-constrained systems. We derive closed-form expressions for the outage probabilities (OPs) of CNOMA users and the intercept probability (IP) of eavesdroppers. Furthermore, closed-form expressions for the detection error probability (DEP) and the average minimum detection error probability (AMDEP) are derived. Finally, an optimization scheme is proposed to maximize the ECR, subject to covertness and security constraints.
3) This research not only provides novel insights into the future advancement of joint covert and secure transmission technologies but also establishes a foundational basis for further developments in this field. To validate the proposed scheme, simulations are conducted to evaluate the covertness and security metrics. Monte Carlo simulations are also performed to compare the theoretical analysis results, demonstrating a high

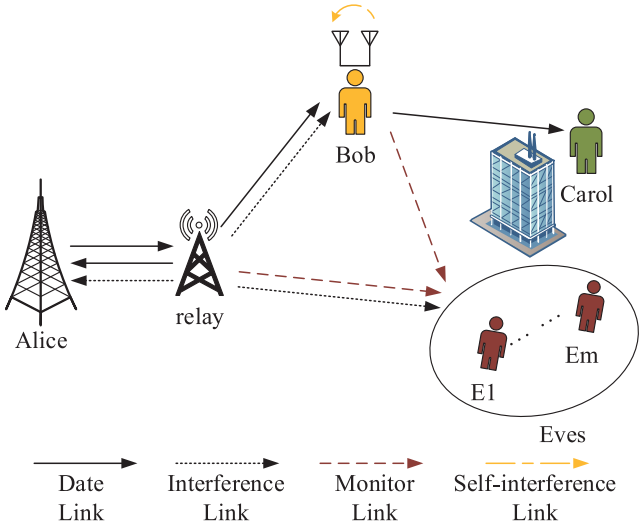

Fig. 1. System model for SWIPT-assisted CNOMA assisted joint covert and secure communication.

degree of consistency between them and further validating the accuracy of the proposed model. The simulation results demonstrate that the maximum ECR, constrained by covertness and security requirements, can be achieved by optimizing the relay's power and power allocation factor.

B. Organization and Notations

The remainder of this article is organized as follows. In Section II, the model of the system and the relate assumptions are described, followed by a discussion on the transmission scheme and the information transmission process. Section III analyzes the performance metrics of the CNOMA users, the warden, and the eavesdroppers. Section IV formulates the optimization scheme to maximize the ECR under covertness and security constraints. Section V presents and discusses the simulation results. Finally, Section VI concludes this article.

Notations: $CN(\mu, \sigma^2)$ represents a complex Gaussian variable with the mean μ and variance σ^2. $\Pr(\cdot)$ and $E(\cdot)$ represent the probability and the expectation for the random variables, respectively. $|\cdot|$ denotes the absolute value of the scalar. $f_x(\cdot)$ and $F_x(\cdot)$ represent the expressions of the probability density function (PDF) and the cumulative distribution function (CDF), respectively.

II. System Model

In this section, the joint covert and secure communication transmission scheme in a SWIPT-assisted CNOMA system is first introduced. Then, we discuss several system-related assumptions, and a list of key system parameters along with their corresponding definitions is provided in Table II. Next, we describe the jamming-assisted and noncolluding eavesdroppers' transmission schemes, and provide a detailed explanation of the information transmission process across different time slots.

A. Model Introduction and Assumptions

We propose a two-hop wireless communication network, as illustrated in Fig. 1. The network consists of a single-antenna transmitter (Alice), a single-antenna greedy relay, a near legitimate user (Bob) equipped with two antennas, a single-antenna far legitimate user (Carol), and multiple single-antenna noncolluding eavesdroppers (Eves).

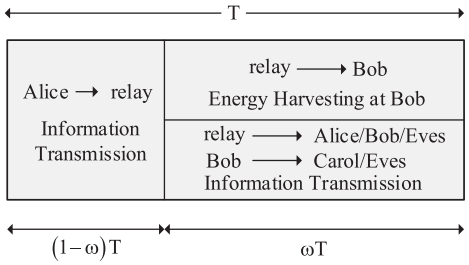

Fig. 2. Process for information transmission and EH.

In the first phase, Alice transmits public NOMA signals to the relay. In the second phase, the relay broadcasts both the public NOMA signals and the confidential signal. During this phase, the decode-and-forward (DF) relay also sends a jamming signal with random transmit power to increase the DEP at Alice and decrease the IP at the Eves. Bob, operating in FD mode, uses the energy harvested from the received signals to modify-and-forward (MF) the confidential information to Carol. Meanwhile, Alice continuously monitors whether the relay transmits the confidential signal to Carol or not. Due to the considerable distance between Alice and Eves, significant path loss results in the signals received by Eves from Alice being exceedingly weak and difficult to decode effectively. Additionally, channel fading further complicates Eves' ability to intercept Alice's transmitted information. As a result, Eves only focus on intercepting the confidential information transmitted by the relay and Bob, who are located much closer. Eves could be aware that the confidential signal forwarded by Bob has been modified, the lack of information about the exact difference between the modified and the original confidential signal forces them to discard Bob's modified signal and rely solely on the signal forwarded by the relay to decode the confidential signal. Therefore, the modified signals do not affect with the desired eavesdropping signals at Eves. The corresponding time-division for information transmission and EH is shown in Fig. 2.

Meanwhile, we make the following assumptions for the system model.

1) We adopt an independent quasi-static Rayleigh fading channel model in this article. The channel coefficient between Alice and relay, relay and Alice are denoted as h_{ar} and h_{ra}, respectively. These channel coefficients, follow the distributions of $CN(0, \lambda_{ar})$ and $CN(0, \lambda_{ra})$. Due to channel reciprocity, $h_{ar} = h_{ra}$. The channel coefficients from relay to Bob, Bob to Carol, relay to the mth eavesdropper (Eve), and Bob to the mth Eve are denoted as h_{rb}, h_{bc}, h_{rE_m}, and h_{bE_m}, respectively, and these channel coefficients, follow the distributions of $CN(0, \lambda_{rb})$, $CN(0, \lambda_{bc})$, $CN(0, \lambda_{rE_m})$, and $CN(0, \lambda_{bE_m})$, where $m \in [1, M]$, and M is the number of Eves. The self-interference channel coefficient of Bob is denoted as h_{bb}, which follows the distribution of $CN(0, \lambda_{bb})$. We assume that the variances of the channel coefficients are distance-dependent, specifically: λ_{ar}, λ_{ra}, λ_{rb}, λ_{bc}, λ_{rE_m}, and λ_{bE_m} satisfy $\lambda_{ar} = d_{ar}^{-\alpha}$, $\lambda_{ra} = d_{ra}^{-\alpha}$, $\lambda_{rb} = d_{rb}^{-\alpha}$,

TABLE II
SUMMARY OF SYMBOLS

Symbols	Meaning of Symbols	Symbols	Meaning of Symbols
h_{ar}	The channel coefficient from Alice to relay	h_{ra}	The channel coefficient from relay to Alice
h_{rb}	The channel coefficient from relay to Bob	h_{bc}	The channel coefficient from Bob to Carol
h_{rE_m}	The channel coefficient from relay to mth Eve	h_{bE_m}	The channel coefficient from Bob to mth Eve
h_{bb}	The self-interference channel coefficient of Bob	λ_{bb}	The variance of the channel coefficient h_{bb}
λ_{ar}	The variance of the channel coefficient h_{ar}	λ_{ra}	The variance of the channel coefficient h_{ra}
λ_{rb}	The variance of the channel coefficient h_{rb}	λ_{bc}	The variance of the channel coefficient h_{bc}
λ_{rE_m}	The variance of the channel coefficient h_{rE_m}	λ_{bE_m}	The variance of the channel coefficient h_{bE_m}
d_{ar}	The distance from Alice to relay	d_{ra}	The distance from relay to Alice
d_{rb}	The distance from relay to Bob	d_{bc}	The distance from Bob to Carol
d_{rE_m}	The distance from relay to mth Eve	d_{bE_m}	The distance from Bob to mth Eve
P_a	The transmission power of Alice	P_r	The transmission power of relay
P_j	The jamming power of relay	$P_j^{\max}$	The maximum jamming power of relay
P_b	The transmission power of Bob	n_a	The additive white Gaussian noise (AWGN) at Alice
n_r	The AWGN at relay	n_{b1}	The AWGN at Bob
n_{b2}	The AWGN introduced during RF-to-baseband conversion	n_b	The overall additive noise at Bob
n_c	The AWGN at Carol	n_{E_m}	The AWGN at the mth Eve
s_b	The public signals for Bob	s_c	The public signals for Carol
s	The confidential signal	$\hat{s}_c$	The modified and forwarded signal of Bob corresponding to s_c
$\hat{s}$	The modified and forwarded signal of Bob corresponding to s	s_j	The jamming signal with random power
γ_r^{th}	The predetermined target signal-to-noise ratio (SNR) at relay	γ_b^{th}	The predetermined target SNR at Bob
γ_c^{th}	The predetermined target SNR at Carol	γ_e^{th}	The predetermined target SNR at Eves
M	The number of eavesdroppers	g	The index of the Eve with the maximum channel gain
ρ	The power allocation factor of Bob in the first phase	ρ_1	The power allocation factor of Bob in the second phase
ρ_2	The power allocation factor of Carol's public signal	ρ_3	The power allocation factor of Carol's confidential signal
β	The power split factor	ϕ	The self-interference cancellation factor
η	The energy conversion efficiency	δ	The time difference between the received and transmitted signal at Bob
τ	The predetermined detection threshold	α	The path loss exponent
R	The predetermined target rate for signal $\hat{s}$	ϵ	The covertness constraint
ω	The time allocation factor for energy harvesting	T	The entire transmission time

$\lambda_{bc} = d_{bc}^{-\alpha}$, $\lambda_{rE_m} = d_{rE_m}^{-\alpha}$, and $\lambda_{bE_m} = d_{bE_m}^{-\alpha}$, where d_{ar}, d_{ra}, d_{rb}, d_{bc}, d_{rE_m}, and d_{bE_m} represent the distances from Alice to relay, relay to Alice, relay to Bob, Bob to Carol, relay to the mth Eve, and Bob to the mth Eve, respectively, and α is the path loss exponent.

2) It is assumed that Alice knows the instantaneous CSI for the Alice-to-relay link, while relay knows the instantaneous CSI for the relay-to-Alice and relay-to-Bob links, as well as the statistical CSI for the relay-to-Eves links. Bob is aware of the instantaneous CSI for the Bob-to-Carol link and the statistical CSI for the Bob-to-Eves links. Meanwhile, Eves have knowledge of the instantaneous CSI for the relay-to-Eves and Bob-to-Eves links.

B. Transmission Schemes

1) Jamming-Assisted Transmission: In the proposed system model, to confuse both Alice and the Eves, a random power transmit scheme is applied. The jamming power P_j of the relay follows a continuous uniform distribution over the interval $[0, P_j^{\max}]$, where $P_j^{\max}$ is the maximum jamming power of the relay. The PDF of the jamming power is given by

$$f_{P_j}(x) = \begin{cases} \frac{1}{P_j^{\max}}, & 0 \le x \le P_j^{\max} \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

2) Noncolluding Eavesdroppers: We assume that all the Eves are noncolluding [13], meaning each Eve independently attempts to decode the confidential information without sharing information or their decoding results with other Eves. The channel gain of the noncolluding Eves is represented by the maximum channel gain among them. According to [51], the PDF of the channel gain for the Eves is expressed as

$$f_{\left|h_{kE_g}\right|^2}(x) = \frac{M}{\lambda_{kE_g}} \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m e^{-\frac{(m+1)x}{\lambda_{kE_g}}} \tag{2}$$

where k denoting the node from which the Eves are attempting to intercept information, which could be either the relay or Bob, i.e., $k \in \{r, b\}$. g being the index of the Eve with the maximum channel gain among the M noncolluding Eves.

C. Information Transmission Process

1) First Phase: In the first phase, Alice transmits superimposed public signals of Bob and Carol to the relay. The received signal at the relay at time t_1 can be expressed as

$$y_r(t_1) = \sqrt{P_a} h_{ar} \left(\sqrt{\rho} s_b(t_1) + \sqrt{1-\rho} s_c(t_1) \right) + n_r \tag{3}$$

where P_a representing the transmission power of Alice, s_b and s_c being the public signals for Bob and Carol, respectively, satisfying $E(|s_b|^2) = E(|s_c|^2) = 1$, n_r denoting the additive white Gaussian noise (AWGN) at the relay, distributed as $n_r \sim CN(0, \sigma^2)$, and ρ being the power allocation factor. Noted that more power is allocated to Carol (the weaker user) in the NOMA system, i.e., $\rho \in (0, 0.5)$.

The DF relay first decodes Carol's signal and then decodes Bob's signal using successive interference cancellation (SIC) technology. The signal-to-noise ratios (SNRs) at the relay for decoding s_c and s_b can be expressed as

$$\gamma_{r \to c} = \frac{(1-\rho) P_a |h_{ar}|^2}{\rho P_a |h_{ar}|^2 + \sigma^2} \tag{4}$$

and

$$\gamma_{r\to b}=\frac{\rho P_a|h_{ar}|^2}{\sigma^2} \tag{5}$$

respectively.

2) Second Phase:

a) Received signal at Bob: In the second phase, the relay broadcasts the superimposed public signals for Bob and Carol, along with the confidential signal and the jamming signal, to Bob. Since Bob operates in FD mode, it simultaneously receives and transmits signal, which introduces self-interference. The received signal at Bob at time t_2 can be expressed as

$$\begin{aligned}y_{b1}(t_2)=&\sqrt{P_r}h_{rb}\left(\sqrt{\rho_1}s_b(t_2)+\sqrt{\rho_2}s_c(t_2)+\sqrt{\rho_3}s(t_2)\right)\\&+\sqrt{\phi P_b}h_{bb}\left(\sqrt{1-\rho_3}\hat{s}_c(t_2-\delta)+\sqrt{\rho_3}\hat{s}(t_2-\delta)\right)\\&+\sqrt{P_j}h_{rb}s_j(t_2)+n_{b1}\end{aligned} \tag{6}$$

where P_r and P_b denoting the transmission power of relay and Bob, respectively, P_j being the jamming power of relay. ρ_1, ρ_2, and ρ_3 are the power allocation factors for Bob's public signal, Carol's public signal, and the confidential signal, respectively. To ensure covertness and security, more power is allocated to the confidential signal, i.e., $\rho_3>\rho_2>\rho_1$, $\rho_3\in(0.5,1)$, and $\rho_1+\rho_2+\rho_3=1$. s is the confidential signal, satisfying $E(|s|^2)=1$. $\hat{s}_c$ and $\hat{s}$ are the modified and forwarded signals of Bob corresponding to s_c and s, respectively, satisfying $E(|\hat{s}_c|^2)=E(|\hat{s}|^2)=1$. s_j is the jamming signal with random power, satisfying $E(|s_j|^2)=1$. n_{b1} is the AWGN at Bob, distributed as $CN(0,\sigma_{b1}^2)$, and ϕ is self-interference cancellation factor of Bob with $\phi\in(0,1)$. δ represents the processing delay, which arises because Bob requires time to harvest energy from relay as well as to decode and reencode the received signals. Furthermore, it is important to note that this processing delay does not impact the system performance.

We assume that the legitimate users can remove the jamming signal by sharing the seeds of the jamming signal [52]. After jamming removal, the signal received at Bob can be reexpressed as

$$\begin{aligned}y_{b2}(t_2)=&\sqrt{P_r}h_{rb}\left(\sqrt{\rho_1}s_b(t_2)+\sqrt{\rho_2}s_c(t_2)+\sqrt{\rho_3}s(t_2)\right)\\&+\sqrt{\phi P_b}h_{bb}\left(\sqrt{1-\rho_3}\hat{s}_c(t_2-\delta)+\sqrt{\rho_3}\hat{s}(t_2-\delta)\right)\\&+n_{b1}.\end{aligned} \tag{7}$$

In the EH process, Bob adopts the PS protocol. Specifically, the power of the received signal at Bob is split into two parts: a fraction $\sqrt{\beta}$ of the power is used to harvest energy and the remaining fraction $\sqrt{1-\beta}$ is used to decode information. Here, $\beta\in[0,1]$ is the power split factor.

According to existing EH schemes, the contribution of self-energy recovery is considered negligible [53], and the AWGN is ignored [54]. Therefore, the harvested energy at Bob over a duration of ωT can be expressed as

$$E=\eta\beta\omega T P_r|h_{rb}|^2 \tag{8}$$

where η is the energy conversion efficiency of Bob, and $\eta\in[0,1]$.

It is assumed that the energy harvested at Bob is used solely for decoding and forwarding information, while the power consumption of the circuit is supplied by Bob's own battery. Thus, the transmit power at Bob can be expressed as

$$P_b=\eta\beta P_r|h_{rb}|^2. \tag{9}$$

The signal used by Bob to decode the information can be expressed as

$$\begin{aligned}y_b(t_2)=&\sqrt{(1-\beta)P_r}h_{rb}\left(\sqrt{\rho_1}s_b(t_2)+\sqrt{\rho_2}s_c(t_2)+\sqrt{\rho_3}s(t_2)\right)\\&+\sqrt{(1-\beta)\phi P_b}h_{bb}\left(\sqrt{1-\rho_3}\hat{s}_c(t_2-\delta)+\sqrt{\rho_3}\hat{s}(t_2-\delta)\right)\\&+n_b\end{aligned} \tag{10}$$

where n_b is the overall additive noise, which is the sum of $\sqrt{1-\beta}n_{b1}$ and n_{b2}, and follows the distribution $n_b\sim CN(0,\sigma^2)$. n_{b2} denotes the AWGN introduced during the conversion of the RF-band signal to the baseband signal, and follows the distribution $n_{b2}\sim CN(0,\sigma_{b2}^2)$. Compared to the AWGN n_{b1}, the processing noise n_{b2} is more dominant [55]. Therefore, we can approximate $\sigma^2\approx\sigma_{b2}^2$.

According to the SIC strategy, the decoding order is expressed as follows: first the confidential signal s, then the public signal s_c, and finally the public signal s_b. The signal to interference plus noise ratios (SINRs) at Bob for decoding s, s_c, and s_b can be denoted as

$$\gamma_{b\to r}=\frac{(1-\beta)\rho_3P_r|h_{rb}|^2}{(1-\beta)\left((\rho_1+\rho_2)P_r|h_{rb}|^2+\phi P_b|h_{bb}|^2\right)+\sigma^2} \tag{11}$$

$$\gamma_{b\to c}=\frac{(1-\beta)\rho_2P_r|h_{rb}|^2}{(1-\beta)\left(\rho_1P_r|h_{rb}|^2+\phi P_b|h_{bb}|^2\right)+\sigma^2} \tag{12}$$

and

$$\gamma_{b\to b}=\frac{(1-\beta)\rho_1P_r|h_{rb}|^2}{(1-\beta)\phi P_b|h_{bb}|^2+\sigma^2} \tag{13}$$

respectively.

b) Received signal at Carol: Due to the presence of an obstacle between the relay and Carol, the signal received at Carol is only transmitted by Bob. Then, the signal received at Carol at time t_2 can be formulated as

$$y_c(t_2)=\sqrt{P_b}h_{bc}\left(\sqrt{1-\rho_3}\hat{s}_c(t_2-\delta)+\sqrt{\rho_3}\hat{s}(t_2-\delta)\right)+n_c \tag{14}$$

where n_c is the AWGN at Carol, distributed as $n_c\sim CN(0,\sigma^2)$.

The SNRs at Carol for decoding $\hat{s}$ and $\hat{s}_c$ are given by

$$\gamma_{c\to r}=\frac{\rho_3P_b|h_{bc}|^2}{(1-\rho_3)P_b|h_{bc}|^2+\sigma^2} \tag{15}$$

and

$$\gamma_{c\to c}=\frac{(1-\rho_3)P_b|h_{bc}|^2}{\sigma^2} \tag{16}$$

respectively.

c) Received signal at Alice: For Alice, it is crucial to determine whether the relay secretly transmits the confidential signal while forwarding the public signals. To achieve this, Alice performs binary hypothesis testing based on its observations: the null hypothesis H_0 indicates that the relay does not transmit the confidential signal, while the alternative hypothesis H_1 suggests that the relay is transmitting the confidential signal.

The corresponding signal received at Alice can be expressed as

$$y_a(t_2) = \begin{cases} \sqrt{P_r}h_{ra}\left(\sqrt{\rho_1}s_b(t_2) + \sqrt{\rho_2}s_c(t_2)\right) \\ +\sqrt{P_j}h_{ra}s_j(t_2) + n_a, & H_0 \\ \sqrt{P_r}h_{ra}\left(\sqrt{\rho_1}s_b(t_2) + \sqrt{\rho_2}s_c(t_2) + \sqrt{\rho_3}s(t_2)\right) \\ +\sqrt{P_j}h_{ra}s_j(t_2) + n_a, & H_1 \end{cases} \tag{17}$$

where n_a represents the AWGN at Alice, distributed as $n_a \sim CN(0, \sigma^2)$.

The average signal power at Alice is defined as $T_a = \sum_{t_2=1}^{T} |y_a(t_2)|^2/T$. When the total time is assumed to be infinite, i.e., $T \to \infty$. Then, the average signal power at Alice can be calculated as

$$T_a = \begin{cases} (\rho_1 + \rho_2)P_r|h_{ra}|^2 + P_j|h_{ra}|^2 + \sigma^2, & H_0 \\ P_r|h_{ra}|^2 + P_j|h_{ra}|^2 + \sigma^2, & H_1. \end{cases} \tag{18}$$

For Alice, it employs a radiometer to detect the presence of the confidential signal. The Neyman-Pearson criterion is used to decide whether covert communication has taken place. The decision rule can be expressed as

$$T_a \underset{D_0}{\overset{D_1}{\gtrless}} \tau \tag{19}$$

where τ is a predetermined detection threshold for the radiometer adopted by Alice. D_0 and D_1 represent Alice's decisions in favor of the null hypothesis H_0 and the alternative hypothesis H_1, respectively.

d) Received signal at Eves: For Eves, decoding the modified signal transmitted by Bob is not feasible [56]. Eves can only intercept the broadcast signal from the relay. The received signal at the mth Eve is given by

$$y_{E_m} = \sqrt{P_r}h_{rE_m}\left(\sqrt{\rho_1}s_b[t_2] + \sqrt{\rho_2}s_c[t_2] + \sqrt{\rho_3}s[t_2]\right) + \sqrt{P_j}h_{rE_m}s_j[t_2] + n_{E_m} \tag{20}$$

where n_{E_m} represents the AWGN at the mth Eve, which follows the distribution $n_{E_m} \sim CN(0, \sigma^2)$.

The signal to interference plus noise ratio (SINR) of the mth Eve is obtained as

$$\gamma_{E_m} = \frac{\rho_3 P_r \left|h_{rE_m}\right|^2}{(\rho_1 + \rho_2)P_r\left|h_{rE_m}\right|^2 + P_j\left|h_{rE_m}\right|^2 + \sigma^2}. \tag{21}$$

Furthermore, since the noncolluding scheme is adopted by the Eves, the SINR for the Eves can be formulated as

$$\gamma_E = \max_{m\in\{1,\ldots,M\}}\left(\gamma_{E_m}\right). \tag{22}$$

III. Performance Analysis

In this section, we analyze the performance of the proposed system from both security and covertness perspectives. First, we investigate the OPs for Bob and Carol, followed by the derivation of the IP for Eves. We then explore the DEP and AMDEP for Alice.

A. Secure Performance Analysis

1) Outage Probability at Bob: For Bob to successfully decode the received signal, two conditions must be satisfied. First the public signals transmitted by Alice must be successfully decoded at the relay. Second, the signal forwarded by the relay must also be successfully decoded at Bob. If either of these conditions is not met, an outage event occurs. The OP for Bob can be expressed as

$$\delta_b = (1 - E_r) + E_r(1 - E_b) \tag{23}$$

where E_r and E_b represent the probabilities of successful decoding of the signals at relay and Bob, respectively. The expressions for E_r and E_b are given by

$$E_r = \Pr\left(\gamma_{r\to c} > \gamma_c^{\text{th}}, \gamma_{r\to b} > \gamma_b^{\text{th}}\right) \tag{24}$$

and

$$E_b = \Pr\left(\gamma_{b\to r} > \gamma_r^{\text{th}}, \gamma_{b\to c} > \gamma_c^{\text{th}}, \gamma_{b\to b} > \gamma_b^{\text{th}}\right) \tag{25}$$

respectively, where γ_rth, γ_bth, and γ_cth are the predetermined target SNRs at relay, Bob, and Carol, respectively.

Theorem 1: The probability that relay successfully decodes the public signals transmitted by Alice is given by

$$E_r = e^{-\frac{\vartheta_1\sigma^2}{\lambda_{ar}P_a}} \tag{26}$$

where $\vartheta_1 = \max([\gamma_b^{\text{th}}/\rho], [\gamma_c^{\text{th}}/(1-\rho) - \rho\gamma_c^{\text{th}}])$.

Proof: By substituting (4) and (5) into (24), the probability that relay successfully decodes the information is written as

$$E_r = \int_{\frac{\vartheta_1\sigma^2}{P_a}}^{\infty} f_{|h_{ar}|^2}(x)dx. \tag{27}$$

■

Theorem 2: The probability that Bob successfully decodes the information received from relay is expressed as

$$E_b \approx e^{-\frac{\sigma^2}{\lambda_{rb}\vartheta_2(1-\beta)P_r}} - \frac{\pi S_1}{2\lambda_{rb}N_1}e^{-\frac{\vartheta_2}{\lambda_{bb}\phi\eta\beta}} \cdot \sum_{n_1=0}^{N_1} e^{\frac{2\sigma^2}{\lambda_{bb}(1-\beta)\phi\eta\beta P_r S_1(\delta_{n1}+1)}} e^{-\frac{S_1(\delta_{n1}+1)}{2\lambda_{rb}}}\sqrt{1-\delta_{n1}^2} \tag{28}$$

where $\vartheta_2 = \min([\rho_1/\gamma_b^{\text{th}}], [\rho_2/\gamma_c^{\text{th}}] - \rho_1, [\rho_3/\gamma_r^{\text{th}}] - (\rho_1 + \rho_2))$, $S_1 = Q_1 - [\sigma^2/\vartheta_2(1-\beta)P_r]$, $\delta_{n1} = \cos[(2n_1 - 1)\pi/2N_1]$, and N_1 is a complexity–accuracy tradeoff parameter.

Proof: By substituting (11)–(13) into (25), the probability that Bob successfully decodes the information is written as

$$E_b = \int_{\frac{\sigma^2}{\vartheta_2(1-\beta)P_r}}^{\infty} \int_0^{\frac{\vartheta_2(1-\beta)P_r y-\sigma^2}{(1-\beta)\phi\eta\beta P_r y}} f_{|h_{bb}|^2}(x) f_{|h_{rb}|^2}(y) dxdy. \quad (29)$$

■

Corollary 1: The asymptotic expression of OP for Bob at high SNR can be expressed as

$$\delta_b^{\infty} \approx 1 + R_1 \sum_{n_1=0}^{N_1} \left(1 + \frac{(\delta_{n1}+1)}{2\lambda_{rb}\vartheta_2(1-\beta)\gamma}\right) e^{-\frac{Q_1(\delta_{n1}+1)}{2\lambda_{rb}}} \sqrt{1-\delta_{n1}^2} + R_1 \sum_{n_1=0}^{N_1} \frac{2\left(1+\frac{(\delta_{n1}+1)}{2\lambda_{rb}\vartheta_2(1-\beta)\gamma}\right)}{\lambda_{bb}(1-\beta)\phi\eta\beta\left(\gamma Q_1 - \frac{1}{\vartheta_2(1-\beta)}\right)(\delta_{n1}+1)} e^{-\frac{Q_1(\delta_{n1}+1)}{2\lambda_{rb}}} \sqrt{1-\delta_{n1}^2} - \left(1-\frac{\vartheta_1}{\lambda_{ar}\gamma}\right)\left(1-\frac{1}{\lambda_{rb}\vartheta_2(1-\beta)\gamma}\right) \quad (30)$$

where $R_1 = [\pi Q_1/2\lambda_{rb}N_1](1-[\vartheta_1/\lambda_{ar}\gamma])e^{-[\vartheta_2/\lambda_{bb}\phi\eta\beta]}$.

Proof: We define the transmit SNR as $\gamma = P/\sigma^2$, where the transmit power P includes P_a and P_r. By applying the approximation $e^{-x} \approx 1-x$ when $x \to 0$, the proof can be completed. ■

2) Outage Probability at Carol: Since the transmission of the confidential signal does not depend on the relay's decoding of the public signal, the success or failure of this decoding has no impact on the confidential signal's transmission. As a result, the failure of the relay to decode the public signal is excluded from the analysis of Carol's OP. For the confidential information to be successfully decoded at Carol, the following two conditions must be met: first, the confidential signal transmitted by the relay must be successfully decoded at Bob. Second, the confidential signal forwarded by Bob must be successfully decoded at Carol. If either of these conditions is not met, an outage event will occur. Therefore, the OP for Carol can be denoted as

$$\delta_c = 1 - \Pr\left(\gamma_{b\to r} > \gamma_r^{\text{th}}, \gamma_{c\to r} > \gamma_r^{\text{th}}\right). \quad (31)$$

Theorem 3: The OP at Carol can be expressed as

$$\delta_c \approx 1 - \left(\frac{\pi S_2}{2\lambda_{bb}N_2}\sum_{n_2=0}^{N_2} k_3 e^{-\frac{\gamma_r^{\text{th}}\sigma^2}{(1-\beta)P_r\lambda_{rb}\left(v-\gamma_r^{\text{th}}\phi\eta\beta k_1\right)}} e^{-\frac{k_1}{\lambda_{bb}}}\right) \cdot \left(\frac{\pi Q_2}{2\lambda_{bc}N_3}\sum_{n_3=0}^{N_3} k_4 e^{-\frac{\gamma_r^{\text{th}}\sigma^2}{\lambda_{rb}\left(\rho_3-\gamma_r^{\text{th}}(1-\rho_3)\right)\eta\beta P_r k_2}} e^{-\frac{k_2}{\lambda_{bc}}}\right) \quad (32)$$

where $S_2 = [\rho_3 - \gamma_r^{\text{th}}(\rho_1+\rho_2)/\gamma_r^{\text{th}}\phi\eta\beta]$, $\delta_{n2} = \cos[(2n_2-1)\pi/2N_2]$, $\delta_{n_3} = \cos[(2n_3-1)\pi/2N_3]$, $k_1 = [S_2(\delta_{n2}+1)/2]$, $k_2 = [Q_2(\delta_{n_3}+1)/2]$, $k_3 = \sqrt{1-\delta_{n2}^2}$, $k_4 = \sqrt{1-\delta_{n_3}^2}$, $v = \rho_3 - \gamma_r^{\text{th}}(\rho_1+\rho_2)$. Here, N_2 and N_3 are complexity–accuracy tradeoff parameters.

Proof: See Appendix A. ■

Corollary 2: The asymptotic expression of OP for Carol at high SNR can be expressed as

$$\delta_c^{\infty} \approx 1 - \frac{\pi Q_2}{2\lambda_{bc}N_3}\sum_{n_3=0}^{N_3}\left(1-\frac{2\gamma_r^{\text{th}}}{\lambda_{rb}(\rho_3-\gamma_r^{\text{th}}(1-\rho_3))\eta\beta\gamma Q_2(\delta_{n_3}+1)}\right)\cdot R_{n2} \cdot \frac{\pi S_2}{2\lambda_{bb}N_2}\sum_{n_2=0}^{N_2}\left(1-\frac{\gamma_r^{\text{th}}}{(1-\beta)\gamma\lambda_{rb}(\rho_3-\gamma_r^{\text{th}}(\rho_1+\rho_2)-\frac{\gamma_r^{\text{th}}\phi\eta\beta S_2(\delta_{n2}+1)}{2})}\right)\cdot R_{n3} \quad (33)$$

where $R_{n2} = e^{-[S_2(\delta_{n2}+1)/2\lambda_{bb}]}\sqrt{1-\delta_{n2}^2}$, $R_{n3} = e^{-[Q_2(\delta_{n_3}+1)/2\lambda_{bc}]}\sqrt{1-\delta_{n_3}^2}$.

Proof: By applying the approximation $e^{-x} \approx 1-x$ when $x \to 0$, the proof can be completed. ■

With the purpose of deeper exploring the performance of the proposed system, the diversity orders of Bob and Carol are discussed. The diversity order is expressed as

$$d = -\lim_{\gamma\to\infty}\frac{\log(\delta^{\infty})}{\log\gamma}. \quad (34)$$

Corollary 3: The diversity orders of Bob and Carol can be expressed as

$$d_b = d_c = 0. \quad (35)$$

Remark 1: From Theorems 1–3 and Corollaries 1–3, it is observed that an increase in SNR leads to a decrease in OPs, thereby improving the system's reliability. Furthermore, the asymptotic OPs exhibit error floors in high-SNR regions, which results in zero diversity order.

3) Intercept Probability at Eavesdroppers: In the presence of noncolluding eavesdroppers, the IP refers to the probability that the Eves successfully intercept the confidential information. For Eves, if their SINRs exceed the predetermined target SNR, the desired information will be successfully intercepted. The IP for the Eves can be expressed as

$$\delta_e = \Pr\left\{\gamma_E > \gamma_e^{\text{th}}\right\} \quad (36)$$

where γ_eth is the predetermined target SNR at the Eves.

Theorem 4: The IP at Eves can be given by

$$\delta_e \approx \frac{\pi S_3}{2N_4}\sum_{n_4=0}^{N_4} e^{-\frac{\sigma^2}{\lambda_{rE_g}(S_3-k_5)}}\sum_{k=0}^{M-1}\frac{k_6(M-1)!}{k!\lambda_{rE_g}^{k-M}}\left[\frac{\sigma^2}{S_3-k_5}\right]^k \quad (37)$$

where $S_3 = ([\rho_3 P_r - \gamma_e^{\text{th}}(\rho_1+\rho_2)P_r]/\gamma_e^{\text{th}})$, $\delta_{n_4} = \cos[(2n_4-1)\pi/2N_4]$, $k_5 = [S_3(\delta_{n_4}+1)/2]$, $k_6 = \sqrt{1-\delta_{n_4}^2}$. Here, N_4 is a complexity-accuaracy tradeoff parameter.

Proof: By substituting (22) into (36), the expression for the IP at Eves can be written as

$$\delta_e = \int_0^{\frac{k_7}{\gamma_e^{\text{th}}}}\int_{\frac{\gamma_e^{\text{th}}\sigma^2}{k_7-\gamma_e^{\text{th}}y}}^{\infty} f_{\left|h_{rE_g}\right|^2}(x) f_{P_j}(y) dxdy \quad (38)$$

where $k_7 = \rho_3 P_r - \gamma_e^{\text{th}}(\rho_1+\rho_2)P_r$. ■

B. Covert Performance Analysis

The DEP is used to assess the detection performance at Alice. When the prior probability for covert transmission is set to 1/2, the DEP can be expressed as

$$\xi = P_{FA} + P_{MD} \quad (39)$$

where $P_{FA} = \Pr(D_1|H_0)$ represents the false alarm probability (FAP), and $P_{MD} = \Pr(D_0|H_1)$ is the missed detection probability (MDP).

The detailed expression for the FAP can be expressed as

$$\begin{aligned} P_{FA} &= \Pr\{T_a > \tau | H_0\} \\ &= \Pr\left\{|h_{ra}|^2 > \frac{\tau - \sigma^2}{(\rho_1+\rho_2)P_r + P_j}\right\} \\ &= \begin{cases} 1, & \tau < \sigma^2 \\ e^{-\frac{\tau-\sigma^2}{\lambda_{ra}((\rho_1+\rho_2)P_r+P_j)}}, & \tau \geq \sigma^2. \end{cases} \end{aligned} \tag{40}$$

Similarly, the expression for MDP can also be derived as

$$\begin{aligned} P_{MD} &= \Pr\left\{P_r|h_{ra}|^2 + P_j|h_{ra}|^2 + \sigma^2 < \tau\right\} \\ &= \Pr\left\{|h_{ra}|^2 < \frac{\tau - \sigma^2}{P_r + P_j}\right\} \\ &= \begin{cases} 0, & \tau < \sigma^2 \\ 1 - e^{-\frac{\tau-\sigma^2}{\lambda_{ra}(P_r+P_j)}}, & \tau \geq \sigma^2. \end{cases} \end{aligned} \tag{41}$$

Substituting (40) and (41) into (39), the DEP at Alice can be given as

$$\xi = \begin{cases} 1, & \tau < \sigma^2 \\ 1 - e^{-\frac{\tau-\sigma^2}{\lambda_{ra}(P_r+P_j)}} + e^{-\frac{\tau-\sigma^2}{\lambda_{ra}((\rho_1+\rho_2)P_r+P_j)}}, & \tau \geq \sigma^2. \end{cases} \tag{42}$$

Theorem 5: The optimal detection threshold for Alice, aimed at minimizing the DEP, can be expressed as

$$\begin{aligned} \tau^* = &\frac{\lambda_{ra}(P_r+P_j)((\rho_1+\rho_2)P_r+P_j)}{(\rho_1+\rho_2-1)P_r} \\ &\cdot \ln\frac{(\rho_1+\rho_2)P_r+P_j}{P_r+P_j} + \sigma^2 \end{aligned} \tag{43}$$

and the MDEP corresponding to the above optimal detection threshold is given by

$$\begin{aligned} \xi^* = 1 &- e^{-\frac{((\rho_1+\rho_2)P_r+P_j)}{(\rho_1+\rho_2-1)P_r}\ln\frac{(\rho_1+\rho_2)P_r+P_j}{P_r+P_j}} \\ &+ e^{-\frac{P_r+P_j}{(\rho_1+\rho_2-1)P_r}\ln\frac{(\rho_1+\rho_2)P_r+P_j}{P_r+P_j}}. \end{aligned} \tag{44}$$

Proof: See Appendix B. ∎

The instantaneous jammer power of the relay is unknown to Alice. Therefore, the expected value of the MDEP, which evaluates the covert performance between the relay and Carol, is derived over all possible realizations of P_j. The AMDEP for Alice is expressed in the following lemma.

Theorem 6: The AMDEP of Alice is denoted as

$$\begin{aligned} \bar{\xi}^* \approx \frac{\pi}{2N_5}\sum_{n_5=0}^{N_5}\sqrt{1-\delta_{n_5}^2}\Bigg(&1 - e^{-\frac{((\rho_1+\rho_2)P_r+S_4)}{(\rho_1+\rho_2-1)P_r}\ln\frac{(\rho_1+\rho_2)P_r+S_4}{P_r+S_4}} \\ &+ e^{-\frac{P_r+S_4}{(\rho_1+\rho_2-1)P_r}\ln\frac{(\rho_1+\rho_2)P_r+S_4}{P_r+S_4}}\Bigg) \end{aligned} \tag{45}$$

where $S_4 = [P_j^{\max}(\delta_{n_5}+1)/2]$, $\delta_{n_5} = \cos[(2n_5-1)\pi/2N_5]$. Here, N_5 is a complexity-accuaracy tradeoff parameter.

Proof: From the MDEP, the AMDEP of Alice can be expressed as

$$\begin{aligned} \bar{\xi}^* &= E[\xi^*] \\ &= \frac{1}{P_j^{\max}}\int_0^{P_j^{\max}}\left(1 - e^{-\frac{((\rho_1+\rho_2)P_r+x)}{(\rho_1+\rho_2-1)P_r}\ln\frac{(\rho_1+\rho_2)P_r+x}{P_r+x}}\right)dx \\ &\quad + \frac{1}{P_j^{\max}}\int_0^{P_j^{\max}} e^{-\frac{P_r+x}{(\rho_1+\rho_2-1)P_r}\ln\frac{(\rho_1+\rho_2)P_r+x}{P_r+x}}dx. \end{aligned} \tag{46}$$

∎

By solving this expression, we derive the result presented in (45).

IV. Optimization of Covert and Secure Performance

The goal of the optimization is to determine the confidential signal's optimal power allocation factor ρ_3^* and relay's optimal transmit power P_r^* to maximize the ECR for Carol, while ensuring that the system satisfies several constraints: the covertness constraint at Alice, the noninterruption constraint at Bob, the security constraint at Eves, the power allocation constraint for the confidential information. The optimization objective can thus be formulated as

$$\max_{\rho_3, P_r} \quad \Upsilon = R(1-\delta_c) \tag{47a}$$

$$\text{s.t.} \quad \bar{\xi}^* \geq 1-\varepsilon \tag{47b}$$

$$\delta_b \leq \delta_b^{\text{th}} \tag{47c}$$

$$\delta_e \leq \delta_e^{\text{th}} \tag{47d}$$

$$\rho_3 > \rho_1 + \rho_2 \tag{47e}$$

where R represents the predetermined target rate for signal $\hat{s}$, ε representing the covertness constraint, and δ_bth and δ_eth denote the maximum OP and IP values allowed at Bob and Eves, respectively. Furthermore, it is deduced that $\rho_1+\rho_2 \in (0, 0.5)$. This constraint on $\rho_1+\rho_2$ inherently restricts the range of ρ_1 within the overall power allocation.

During the first iteration, P_r is treated as an arbitrary constant and substituted into the optimization objective and constraints to obtain the power allocation factor ρ_3^1. The detail optimization process for the problem can be given as follows.

a) Optimization process for ρ_3^1: The optimization of the power allocation factor ρ_3^1 follows three steps.

Step 1—Satisfying the Covertness Constraint: Since $\bar{\xi}^*$ decreases monotonically with the increase of ρ_3^1. When the covertness constraint (47b) is satisfied, the range of the power allocation factor can be obtained, and $\rho_3^1 \leq \rho_3'$, where ρ_3' denotes the solution for $\bar{\xi}^* = 1-\varepsilon$.

Step 2—Satisfying the Reliability Constraint: It is observed that δ_b decreases initially and then increases with the increase of ρ_3^1. Therefore, when the reliability constraint (47c) is satisfied, the range of the power allocation factor can be obtained, and $\rho_3'' \leq \rho_3^1 \leq \rho_3'''$, where ρ_3'' and ρ_3''' are the solutions for $\delta_b = \delta_b$th.

Step 3—Satisfying the Security Constraint: Since δ_e is an increasing function with respect to ρ_3^1. When the security constraint (47d) is satisfied, the range of the power allocation factor can be obtained, and $\rho_3^1 \leq \rho_3^\dagger$, where $\rho_3^\dagger$ is the solution for $\delta_e = \delta_e$th.

Since Υ is considered to be an increasing function of ρ_3^1. Based on the analysis of these constraints, we know that there exists a power allocation factor $\rho_3^1 = \min(\rho_3', \rho_3''', \rho_3^\dagger)$ that maximizes the ECR while satisfying the covertness, reliability, security, and power allocation constraints.

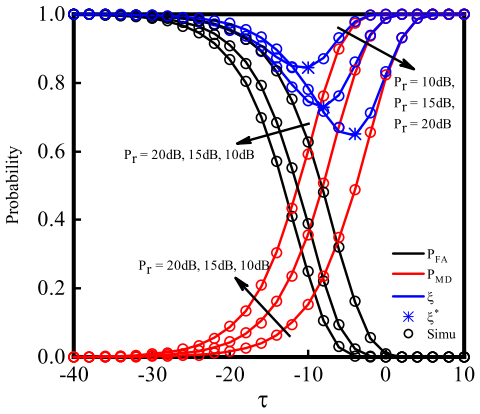

Fig. 3. P_{FA}, P_{MD}, and ξ versus τ for different values of P_r.

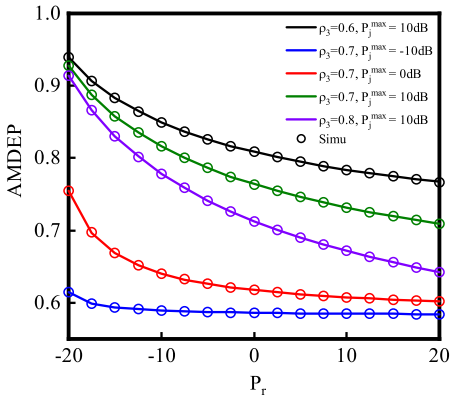

Fig. 4. $\bar{\xi}^*$ versus P_r for different values of ρ_3 and P_j.

b) Optimization process for P_r: Once ρ_3^1 is obtained, it is substituted back into the optimization formulations to derive the corresponding relay's transmit power P_r^1. The optimization process for P_r^1 follows three steps.

Step 1—Satisfying the Covertness Constraint: Since $\bar{\xi}^*$ decreases monotonically with the increase of P_r^1. When the covertness constraint (47b) is satisfied, the range of the relay's transmit power can be obtained, and $P_r^1 \leq P_r{}'$, where $P_r{}'$ denotes the solution for $\bar{\xi}^* = 1 - \varepsilon$.

Step 2—Satisfying the Reliability Constraint: Since δ_b decreases with the increase of P_r^1. When the reliability constraint (47c) is satisfied, the range of the relay's transmit power can be obtained, and $P_r^1 \geq P_r{}''$, where $P_r{}''$ denotes the solution for $\delta_b = \delta_b$th.

Step 3—Satisfying the Security Constraint: It is observed that δ_e increases as P_r^1 increases, When the security constraint (47d) is satisfied, the range of the relay's transmit power can be obtained, and $P_r^1 \leq P_r{}'''$, where $P_r{}'''$ denotes the solution for $\delta_e = \delta_e$th.

Considering that Υ increases with the increase of P_r^1. Thus, the value of the transmit power of the relay can be expressed as $P_r^1 = \min(P_r{}', P_r{}''')$.

In the tth iteration, P_r^{t-1} is substituted into the optimization formulations to compute ρ_3^t, and then ρ_3^t is used to compute P_r^t. This iterative procedure continues until the convergence criteria are satisfied. Through this process, the optimal values ρ_3^* and P_r^* are ultimately obtained. Although this process cannot fully guarantee a global optimal solution due to the interdependence of ρ_3 and P_r, it still provides valuable insights and meaningful results for the current analysis.

V. Numerical Results and Discussion

In this section, we analyze and investigate the covert and secure performance of the system through numerical simulations. The results validate the analytical findings and provide insights into optimization strategies for maximizing the ECR under various constraints. The simulation parameters are set as follows: $d_{ar} = d_{ra} = 12$ m, $d_{rb} = 5$ m, $d_{rE_m} = 15$ m, $d_{bc} = 3$ m, $d_{bE_m} = 8$ m, $\lambda_{bb} = -9$ dB, $\alpha = 2.1$, $M = 4$, $P_a = 20$ dB, $\sigma^2 = -20$ dB, $\gamma_r^{\text{th}} = \gamma_b^{\text{th}} = \gamma_c^{\text{th}} = \gamma_e^{\text{th}} = 1$, and $R = 1$ bps/Hz.

In Fig. 3, we present the trends of the P_{FA} FAP, P_{MD} MDP, and ξ (DEP) versus the detection threshold τ for different values of relay's transmit power P_r. It can be observed that the FAP decreases monotonically from 1 to 0 as the detection threshold τ increases. Conversely, the MDP increases monotonically from 0 to 1 as τ increases. The DEP decreases initially and then increases with the increase of τ, implying that there exists an optimal detection threshold τ^* that minimizes the DEP. Meanwhile, it can be observed that the effect of the relay's power P_r is significant. As P_r decreases, Alice's ability to detect covert communication diminishes, and the optimal detection threshold τ^* becomes smaller. This result is consistent with the analytical findings in (43). The theoretical and simulation curves are in close agreement, validating the accuracy of the derived expressions.

Fig. 4 illustrates the relationship between the AMDEP $\bar{\xi}^*$ and relay's transmit power P_r for different values of the power allocation factor ρ_3 and the maximum jamming power $P_j^{\max}$. It can be observed that AMDEP decreases as P_r increases. This reflects that higher transmission power increases the likelihood of detection by Alice, and as the increase of ρ_3, AMDEP decreases, indicating that more power allocated to the confidential signal increases the chance of detection by Alice. Meanwhile, it can be observed that AMDEP increases with the increase of maximum jamming power values, suggesting that larger jamming power makes it harder for Alice to distinguish between the confidential signal and the jamming signal, thus disturbing Alice's detection capability.

Fig. 5 shows the variation of Bob's OP versus the relay's transmit power P_r for different values of the power split factor β and the distance d_{rb} between the relay and Bob. It can be observed that as P_r increases, the OP of Bob decreases monotonically, indicating that higher transmission power improves Bob's ability to decode the signal, and the OP increases with an increase in β, as a higher β allocates less power to information decoding, resulting in higher chances of outage. Meanwhile, the OP also increases with the distance d_{rb}, suggesting that as the distance between the relay and Bob increases, the quality of the signal received by Bob deteriorates, leading to a higher OP.

In Fig. 6, we present the variation of Bob's OP versus the energy conversion efficiency η for different values of the self-interference cancellation factor ϕ and the variance of Bob's

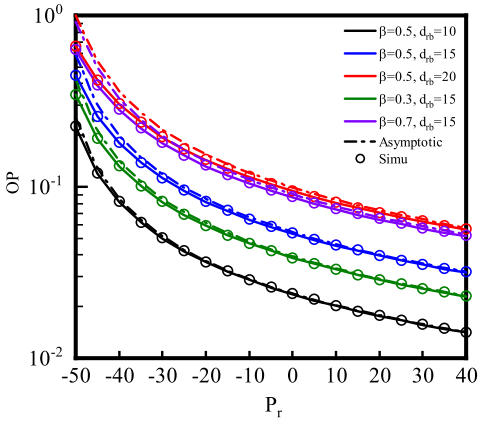

Fig. 5. δ_b versus P_r for different values of β and d_{rb}.

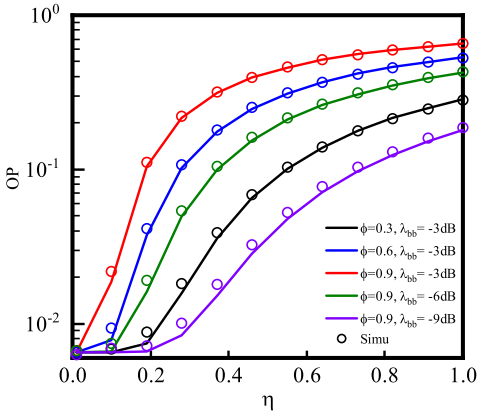

Fig. 6. δ_b versus P_r for different values of ρ_3 and P_j.

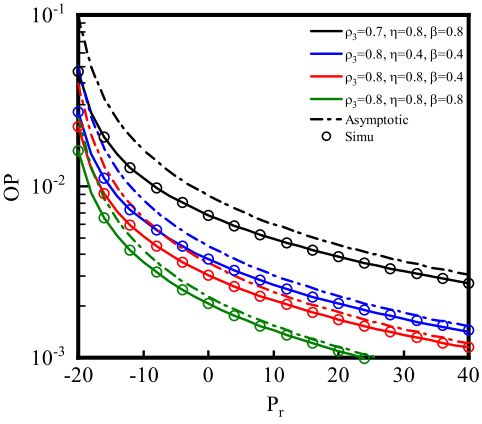

Fig. 7. δ_c versus P_r for different values of ρ_3, η, and β.

self-interference channel coefficient λ_{bb}. It can be observed that Bob's OP increases with the increase of η. Higher energy conversion efficiency enables Bob to harvest more energy, but this also introduces more self-interference during the decoding process, and as ϕ increases, Bob's OP increases, due to the additional interference caused by incomplete self-interference cancellation. Meanwhile, it can be observed that an increase in λ_{bb} also leads to higher OP, as it reflects worse self-interference channel conditions, further hindering Bob's decoding ability.

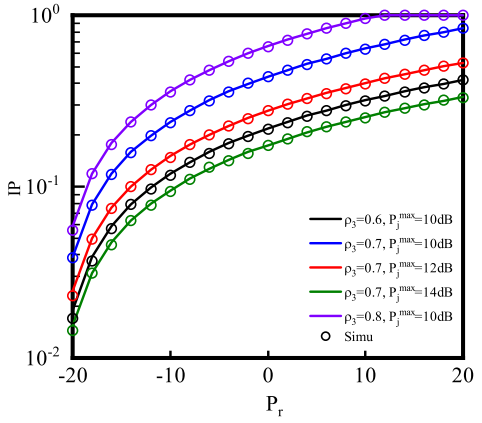

Fig. 8. δ_e versus P_r for different values of ρ_3 and P_j.

Fig. 7 depicts the trends of Carol's OP δ_c versus the relay's transmit power P_r for different values of the power allocation factor ρ_3, energy conversion efficiency η, and power split factor β. It is evident that OP at Carol decreases monotonically as P_r increases. This decrease is attributed to the corresponding increase in Bob's transmission power, which is positively correlated with P_r. The enhancement in p_b leads to a higher probability of successful reception and decoding of the confidential signal by Carol, thereby reducing its OP. Meanwhile, we observe that OP at Carol gradually decreases with an increase in the power allocation factor ρ_3, signifying that a greater proportion of power is allocated to the confidential signal rather than the public signals. This allocation strategy helps reduce the OP at Carol. Furthermore, it can be observed that increasing η or β also leads to a reduction in Carol's OP. Higher η indicates more efficient energy utilization, while higher β reflects more power directed toward confidential signal transmission, both improving Carol's performance.

In Fig. 8, we show the relationship between the δ_e (IP) of Eves and the relay's transmit power P_r for different values of the power allocation factor ρ_3 and maximum jamming power $P_j^{\max}$. It can be observed that the IP of Eves increases as P_r increases, suggesting that higher transmission power raises the chances of successful eavesdropping, and increasing ρ_3 further increases the IP, as more power is allocated to the confidential signal, making it easier for Eves to intercept. Thus, it is crucial to determine the optimal values of ρ_3 and P_r to ensure that covert communication between relay and Carol remains secure from Alice's detection and the potential eavesdropping by Eves. Additionally, the IP decreases with increasing $P_j^{\max}$, indicating that the jamming signal transmitted by the relay effectively reduces the risk of eavesdropping by confusing the Eves.

Fig. 9 demonstrates the variation of the maximum ECR for Carol versus the relay's transmit power P_r for different values of the covertness constraint ε and the energy conversion efficiency η. It can be observed that the maximum ECR increases as P_r increases, showing that higher transmission power enhances the covert communication rate for Carol, and as ε increases, the maximum ECR increases significantly, indicating that a relaxed covertness constraint allows more

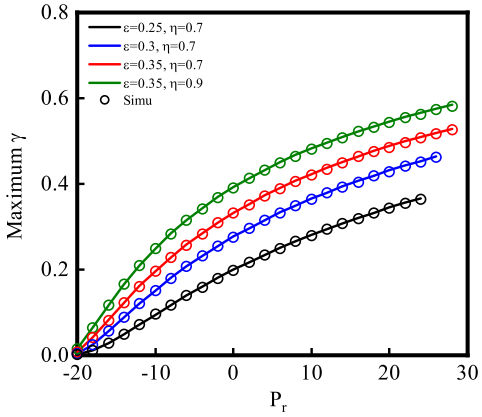

Fig. 9. Maximum Υ versus P_r for different values of ε and η.

confidential information to be transmitted. Meanwhile, it can be observed that the maximum ECR also increases with η. It can be concluded that higher energy conversion efficiency enables more energy to be harvested and used for information transmission, thus improving the ECR. For different values of ε and η, the optimal power P_r^* also changes, resulting in variations in the range of achievable power values.

VI. Conclusion

In this article, we investigated the problem of joint covert and secure communication within a SWIPT-assisted CNOMA system. We derived closed-form expressions for various covert performance metrics, including the DEP, MDEP, and AMDEP. To assess security, we derived closed-form expressions for the OP and IP. Specifically, we jointly designed the power allocation factor for the confidential signal and the transmit power of the relay to maximize the ECR. This optimization was done while ensuring that both covertness and security constraints were satisfied. The results demonstrated that the system's reliability for Carol is significantly enhanced by adopting CNOMA and SWIPT technologies. It has been found that the random power jamming scheme was helpful to assist in covert and secure communication, as jamming signal effectively disrupted the detection and interception efforts of the warden and eavesdroppers. Additionally, the simulation results confirmed that the optimal power allocation factor and the optimal transmission power can maximize the ECR. The proposed system presents a promising solution for enhancing communication covertness and security in energy-constrained situations.

Appendix A

According to (31), the OP at Carol can be written as

$$\delta_c = 1 - \underbrace{\Pr\left(\gamma_{b\to r} > \gamma_r^{\text{th}}\right)}_{I_1} \underbrace{\Pr\left(\gamma_{c\to r} > \gamma_r^{\text{th}}\right)}_{I_2}. \tag{48}$$

where I_1 and I_2 can be expressed as

$$I_1 = \int_0^{\frac{\rho_3-\gamma_r^{\text{th}}(\rho_1+\rho_2)}{\gamma_r^{\text{th}}\phi\eta\beta}} \int_{\frac{\gamma_r^{\text{th}}\sigma^2}{(1-\beta)P_r\left(\nu-\gamma_r^{\text{th}}\phi\eta\beta y\right)}}^{\infty} f_{|h_{rb}|^2}(x) f_{|h_{bb}|^2}(y)dxdy$$

$$\approx \frac{\pi S_2}{2\lambda_{bb}N_2}\sum_{n_2=0}^{N_2} k_3 e^{-\frac{\gamma_r^{\text{th}}\sigma^2}{(1-\beta)P_r\lambda_{rb}\left(\nu-\gamma_r^{\text{th}}\phi\eta\beta k_1\right)}} e^{-\frac{k_1}{\lambda_{bb}}} \tag{49}$$

and

$$I_2 = \int_0^{\infty}\int_{\frac{\gamma_r^{\text{th}}\sigma^2}{\left(\rho_3-\gamma_r^{\text{th}}(1-\rho_3)\right)\eta\beta P_r y}}^{\infty} f_{|h_{rb}|^2}(x) f_{|h_{bc}|^2}(y)dxdy$$

$$\approx \frac{\pi Q_2}{2\lambda_{bc}N_3}\sum_{n_3=0}^{N_3} k_4 e^{-\frac{\gamma_r^{\text{th}}\sigma^2}{\lambda_{rb}\left(\rho_3-\gamma_r^{\text{th}}(1-\rho_3)\right)\eta\beta P_r k_2}} e^{-\frac{k_2}{\lambda_{bc}}} \tag{50}$$

respectively.

Substituting (49) and (50) into (48), we can derive the result (32), thereby completing the proof of the theorem.

Appendix B

According to the expression for the DEP in (42), the optimal detection threshold corresponding to different ranges of the threshold can be determined as follows.

1) When $\tau < \sigma^2$, ξ remains a constant. This implies that no optimal detection threshold exists in this range because the DEP does not change with respect to τ.
2) When $\tau \geq \sigma^2$, the monotonicity of the DEP is not immediately obvious through direct observation. To determine the behavior of the DEP in this case, we compute the derivative of the DEP with respect to τ. The derivative can be expressed as

$$\frac{\partial\xi}{\partial\tau} = \frac{1}{\lambda_{ra}\left(P_r+P_j\right)} e^{-\frac{\tau-\sigma^2}{\lambda_{ra}\left(P_r+P_j\right)}} - \frac{1}{\lambda_{ra}\left((\rho_1+\rho_2)P_r+P_j\right)} e^{-\frac{\tau-\sigma^2}{\lambda_{ra}\left((\rho_1+\rho_2)P_r+P_j\right)}}. \tag{51}$$

Let $(\partial\xi/\partial\tau) = 0$, we can obtain $\tau^\dagger = [\lambda_{ra}(P_r+P_j)((\rho_1+\rho_2)P_r+P_j)/(\rho_1+\rho_2-1)P_r]\ln[(\rho_1+\rho_2)P_r+P_j/(P_r+P_j)] + \sigma^2$. When we select a random threshold τ that satisfies $\tau < \tau^\dagger$, the value of the derivative is less than 0, i.e., $(\partial\xi/\partial\tau) < 0$. Conversely, when we select a random threshold τ that satisfies $\tau > \tau^\dagger$, the value of the derivative is greater than 0, i.e., $(\partial\xi/\partial\tau) > 0$. Therefore, this indicates that the value of DEP decreases first and then increases as τ increases. This means that the value of DEP can be minimize when $\tau = \tau^\dagger$. Therefore, we conclude that the optimal detection threshold satisfies $\tau^* = [\lambda_{ra}(P_r+P_j)((\rho_1+\rho_2)P_r+P_j)/(\rho_1+\rho_2-1)P_r]\ln[(\rho_1+\rho_2)P_r+P_j/(P_r+P_j)] + \sigma^2$.

By substituting this optimal detection threshold τ^* into (42), the corresponding MDEP can be obtained.

References

[1] R. Kaur, B. Bansal, S. Majhi, S. Jain, C. Huang, and C. Yuen, "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 172–199, 2024.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[3] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[4] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[5] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, Feb. 2018.

[6] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.

[7] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4457–4462, May 2017.

[8] Y. Zheng et al., "Overlay cognitive ABCom-NOMA-based ITS: An in-depth secrecy analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2217–2228, Feb. 2023.

[9] X. Li et al., "Cognitive AmBC-NOMA IoV-MTS networks with IQI: Reliability and security analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2596–2607, Feb. 2023.

[10] M. Asif, X. Bao, A. Ihsan, W. U. Khan, M. Ahmed, and X. Li, "Securing NOMA 6G communications leveraging intelligent OMNI-surfaces under residual hardware impairments," *IEEE Internet Things J.*, vol. 11, no. 14, pp. 25326–25336, Jul. 2024.

[11] X. Li, Y. Zheng, M. Zeng, Y. Liu, and O. A. Dobre, "Enhancing secrecy performance for STAR-RIS NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2684–2688, Feb. 2023.

[12] X. Li et al., "Reliability and security of CR-STAR-RIS-NOMA-assisted IoT networks," *IEEE Internet Things J.*, vol. 11, no. 17, pp. 27969–27980, Sep. 2024.

[13] T. M. Hoang, L. T. Dung, B. C. Nguyen, X. N. Tran, and T. Kim, "Secrecy outage performance of FD-NOMA relay system with multiple non-colluding eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12985–12997, Dec. 2021.

[14] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[15] X. Lu, S. Yan, W. Yang, M. Li, and D. W. K. Ng, "Covert communication with time uncertainty in time-critical wireless networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 1116–1129, Feb. 2023.

[16] Y. Zhang et al., "Covert communication in downlink NOMA systems with channel uncertainty," *IEEE Sensors J.*, vol. 22, no. 19, pp. 19101–19112, Oct. 2022.

[17] R. He, G. Li, H. Wang, Y. Jiao, and J. Cai, "Adaptive power control for cooperative covert communication with partial channel state information," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1428–1432, Jul. 2022.

[18] Z. Duan, X. Yang, Y. Gong, D. Wang, and L. Wang, "Covert communication in uplink NOMA systems under channel distribution information uncertainty," *IEEE Commun. Lett.*, vol. 27, no. 5, pp. 1282–1286, May 2023.

[19] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 760–773, 2022.

[20] W. He et al., "Optimal transmission probabilities of information and artificial noise in covert communications," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 2865–2869, Dec. 2022.

[21] Y. Wen et al., "Covert communications aided by cooperative jamming in overlay cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 12878–12891, Dec. 2024.

[22] X. Li et al., "Covert communication of STAR-RIS aided NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 9055–9060, Jun. 2024.

[23] S. Feng, X. Lu, D. Niyato, Y. Wu, S. X. Shen, and W. Wang, "System-level security solution for hybrid D2D communication in heterogeneous D2D-underlaid cellular network," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 15054–15069, Oct. 2024.

[24] Y. Zhang, R. D. Candia, H. Yiğitler, R. Jäntti, and Z. Yan, "Covert backscatter communication in the presence of multi-antenna eavesdropper," *IEEE Commun. Lett.*, vol. 28, no. 8, pp. 1770–1774, Aug. 2024.

[25] M. Forouzesh, P. Azmi, and A. Kuhestani, "Secure transmission with covert requirement in untrusted relaying networks," in *Proc. 9th Int. Symp. Telecommun. (IST)*, 2018, pp. 670–675.

[26] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3737–3749, Jun. 2020.

[27] R. Sun, B. Yang, Y. Shen, X. Jiang, and T. Taleb, "Covertness and secrecy study in untrusted relay-assisted D2D networks," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 17–30, Jan. 2023.

[28] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint information-theoretic secrecy and covert communication in the presence of an untrusted user and warden," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7170–7181, May 2021.

[29] C. Wang, Z. Li, H. Zhang, D. W. K. Ng, and N. Al-Dhahir, "Achieving covertness and security in broadcast channels with finite blocklength," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7624–7640, Sep. 2022.

[30] M. Forouzesh, F. S. Khodadad, P. Azmi, A. Kuhestani, and H. Ahmadi, "Simultaneous secure and covert transmissions against two attacks under practical assumptions," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10160–10171, Jun. 2023.

[31] Y. Yang, S. Shen, Y. She, W. Wang, B. Yang, and Y. Gao, "Joint covert and secure communications for intelligent reflecting surface (IRS)-aided wireless networks," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, 2023, pp. 138–142.

[32] L. Yang et al., "Covert transmission and secrecy analysis of RS-RIS-NOMA-aided 6G wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 10659–10670, Aug. 2023.

[33] P. Chen et al., "Covert transmission and physical-layer security of active RIS-RS-NOMA-aided communication systems," *IEEE Internet Things J.*, vol. 11, no. 19, pp. 31507–31520, Oct. 2024.

[34] H. Xiao et al., "STAR-RIS enhanced joint physical layer security and covert communications for multi-antenna mmWave systems," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8805–8819, Aug. 2024.

[35] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. Int. Symp. Inf. Theory*, 2008, pp. 1612–1616.

[36] O. Maraqa, A. S. Rajasekaran, S. Al-Ahmadi, H. Yanikomeroglu, and S. M. Sait, "A survey of rate-optimal power domain NOMA with enabling technologies of future wireless networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2192–2235, 4th Quart., 2020.

[37] Y. Liu, W. Yi, Z. Ding, X. Liu, O. A. Dobre, and N. Al-Dhahir, "Developing NOMA to next generation multiple access: Future vision and research opportunities," *IEEE Wireless Commun.*, vol. 29, no. 6, pp. 120–127, Dec. 2022.

[38] S. Timotheou and I. Krikidis, "Fairness for non-orthogonal multiple access in 5G systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1647–1651, Oct. 2015.

[39] M. Ghous, A. K. Hassan, Z. H. Abbas, G. Abbas, A. Hussien, and T. Baker, "Cooperative power-domain NOMA systems: An overview," *Sensors*, vol. 22, no. 24, p. 9652, Dec. 2022.

[40] O. Alamu, T. O. Olwal, and K. Djouani, "Cooperative NOMA networks with simultaneous wireless information and power transfer: An overview and outlook," *Alexandria Eng. J.*, vol. 71, pp. 413–438, May 2023.

[41] A. A. Amin and S. Y. Shin, "Investigate the dominating factor of hybrid SWIPT protocol by performance analysis of the far user of hybrid SWIPT based CNOMA downlink transmission," in *Proc. Int. Conf. Electr. Comput. Commun. Eng. (ECCE)*, 2019, pp. 1–6.

[42] X. Yin, W. Wu, H. Dai, P. Li, and B. Wang, "Energy-efficient transceiver design for full-duplex cooperative NOMA systems with SWIPT," in *Proc. 10th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2018, pp. 1–6.

[43] Z. Zhang, H. Qu, J. Zhao, W. Wang, and S. Wang, "Fairness based power allocation optimization of cooperative NOMA with SWIPT network," in *Proc. IEEE 4th Int. Conf. Signal Image Process. (ICSIP)*, 2019, pp. 555–560.

[44] Y. Ye, Y. Li, D. Wang, and G. Lu, "Power splitting protocol design for the cooperative NOMA with SWIPT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2017, pp. 1–5.

[45] R. Lei and D. Xu, "On the outage performance of JT-CoMP-CNOMA networks with SWIPT," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 432–436, Feb. 2021.

[46] A. S. Parihar, P. Swami, and V. Bhatia, "On performance of SWIPT enabled PPP distributed cooperative NOMA networks using stochastic geometry," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 5639–5644, Feb. 2022.

[47] T.-T. Nguyen, S. Q. Nguyen, P. X. Nguyen, and Y.-H. Kim, "Evaluation of full-duplex SWIPT cooperative NOMA-based IoT relay networks over Nakagami-*m* fading channels," *Sensors*, vol. 22, no. 5, p. 1974, 2022.

[48] A. Baranwal, S. Sharma, S. D. Roy, and S. Kundu, "On performance of a full duplex SWIPT enabled cooperative NOMA network," *Wireless Netw.*, vol. 30, no. 3, pp. 1643–1656, Apr. 2024.

[49] D. P. P. R. Baduge, T. D. P. Perera, and D. N. K. Jayakody, "Flight to efficiency: Trajectory optimization in SWIPT-enabled UAV-assisted NOMA for future wireless networks," in *Proc. IEEE 100th Veh. Technol. Conf. (VTC-Fall)*, Washington, DC, USA, 2024, pp. 1–7.
[50] X. Sun, W. Yang, and Y. Cai, "Secure communication in NOMA-assisted millimeter-wave SWIPT UAV networks," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1884–1897, Mar. 2020.
[51] K. Shim, T.-V. Nguyen, and B. An, "Exploiting opportunistic scheduling schemes to improve physical-layer security in MU-MISO NOMA systems," *IEEE Access*, vol. 7, pp. 180867–180886, 2019.
[52] R. Chen, J. Yang, H. Zhou, R. Lu, and D. Zeng, "Covert communication in two-hop cooperative cognitive radio system," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16567–16581, Dec. 2023.
[53] Y. Zeng and R. Zhang, "Full-duplex wireless-powered relay with self-energy recycling," *IEEE Wireless Commun. Lett.*, vol. 4, no. 2, pp. 201–204, Apr. 2015.
[54] H. Liu, K. J. Kim, K. S. Kwak, and H. V. Poor, "Power splitting-based SWIPT with decode-and-forward full-duplex relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7561–7577, Nov. 2016.
[55] K. Agrawal, M. F. Flanagan, and S. Prakriya, "NOMA with battery-assisted energy harvesting full-duplex relay," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13952–13957, Nov. 2020.
[56] S.-I. Chu, "Secrecy analysis of modify-and-forward relaying with relay selection," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1796–1809, Feb. 2019.

Gaojian Huang (Member, IEEE) received the bachelor's degree in electronic information engineering and the Ph.D. degree in information and communications engineering from Guilin University of Electronic Technology, Guilin, China, in 2013 and 2021, respectively.

From October 2017 to October 2018, he was a Visiting Researcher with Queen's University Belfast, Belfast, U.K. He is currently a Lecturer with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China. His research interests include integrated sensing and wireless communication designs, antenna array, physical-layer security, emerging modulation techniques, and 5G/6G related areas.

Yuxin Lei received the B.Sc. degree in electronic information engineering from the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China, in 2022, where she is currently pursuing the M.Sc. degree in electronic information.

Her current research interests include NOMA, STAR-RIS, and physical-layer security.

Xingwang Li (Senior Member, IEEE) received the M.Sc. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2010, and the Ph.D. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2015.

From 2010 to 2012, he was working with Comba Telecom Ltd., Guangzhou, China, as an Engineer. He was a Visiting Scholar with Queen's University Belfast, Belfast, U.K., from 2017 to 2018. He is currently an Associate Professor with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China. His research interests span wireless communication, intelligent transport system, artificial intelligence, and Internet of Things.

Dr. Li is on the editorial board of IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS LETTERS, and IEEE SYSTEMS JOURNAL.

Wali Ullah Khan (Member, IEEE) received the master's degree in electrical engineering from COMSATS University Islamabad, Islamabad, Pakistan, in 2017, and the Ph.D. degree in information and communication engineering from Shandong University, Qingdao, China, in 2020.

He is currently working with the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Esch-sur-Alzette, Luxembourg. He has authored/co-authored more than 50 publications, including international journals, peer reviewed conferences, and book chapters. His research interests include convex/non-convex optimizations, non-orthogonal multiple access, reflecting intelligent surfaces, ambient backscatter communications, Internet of Things, intelligent transportation systems, satellite communications, physical-layer security, and applications of machine learning.

Gongpu Wang (Senior Member, IEEE) received the B.Eng. degree in communication engineering from Anhui University, Hefei, China, in 2001, the M.Sc. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2004, and the Ph.D. degree from the University of Alberta, Edmonton, AB, Canada, in 2011.

From 2004 to 2007, he was an Assistant Professor with the School of Network Education, Beijing University of Posts and Telecommunications. He is currently a Full Professor with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing. His research interests include wireless communication, signal processing, and Internet of Things.

Arumugam Nallanathan (Fellow, IEEE) received the B.Eng. degree (Hons.) in electrical and electronic engineering from the University of Peradeniya, Galaha, Sri Lanka, in 1991, the CPGS degree in electrical and electronic engineering from the University of Cambridge, Cambridge, U.K., in 1994, and the Ph.D. degree in electrical and electronic engineering from the University of Hong Kong, Hong Kong, in 2000.

He has been a Professor of Wireless Communications and the Head of the Communication Systems Research Group, School of Electronic Engineering and Computer Science, Queen Mary University of London, London, U.K., since September 2017. He was with the Department of Informatics, KingŠs College London, London, from December 2007 to August 2017, where he was a Professor of Wireless Communications from April 2013 to August 2017 and a Visiting Professor from September 2017 to August 2020. He was an Assistant Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, from August 2000 to December 2007. He published more than 700 technical papers in scientific journals and international conferences. His research interests include artificial intelligence for wireless systems, beyond 5G wireless networks, and Internet of Things.

Prof. Nallanathan is a co-recipient of the Best Paper Awards presented at the IEEE International Conference on Communications 2016 (ICCŠ2016), IEEE Global Communications Conference 2017 (GLOBECOMŠ2017), and IEEE Vehicular Technology Conference 2018 (VTCŠ2018). He is also a co-recipient of IEEE Communications Society Leonard G. Abraham Prize in 2022. He has been selected as a Web of Science Highly Cited Researcher in 2016 and from 2022 to 2024. He received the IEEE Communications Society SPCE Outstanding Service Award in 2012 and the IEEE Communications Society RCC Outstanding Service Award in 2014. He was a Senior Editor for IEEE WIRELESS COMMUNICATIONS LETTERS, an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE SIGNAL PROCESSING LETTERS. He served as the Chair for the Signal Processing and Communication Electronics Technical Committee of IEEE Communications Society and the Technical Program Chair and the member of Technical Program Committees in numerous IEEE conferences. He is an IEEE Distinguished Lecturer.