PLOS ONE

RESEARCH ARTICLE

# Enhancing covert communication in NOMA systems with joint security and covert design

**Thanh Binh Doan**[1], **Tien-Hoa Nguyen**[2]*

**1** Department of Electronics and Telecommunications, Electric Power University, Hanoi, Vietnam, **2** School of Electrical and Electronic Engineering, Hanoi University of Science and Technology, Hanoi, Vietnam

* hoa.nguyentien@hust.edu.vn

## Abstract

The explosion of Internet-of-Thing enables several interconnected devices but also gives rise chance for unauthorized parties to compromise sensitive information through wireless communication systems. Covert communication therefore has emerged as a potential candidate for ensuring data privacy in conjunction with physical layer transmission to render two lines of defense. In this paper, we aim to enhance the individual transmission of nearby users in non-orthogonal multiple access (NOMA) systems under scenarios of an eavesdropper who monitors covert transmission before decoding covert information. For this problem, we first provide a comprehensive analysis of the NOMA system in terms of outage probability (OP), secrecy outage probability (SOP), and detection error probability (DEP), where all of them are quantified in exact and asymptotic closed-form expressions. Besides, we have also derived closed-form formulas for users' covert and public rates. Under the system requirements of the maximal OP and SOP and the minimal DEP, we formulate the optimization of resource power allocation to: 1) minimize the OP of covert communication and 2) maximize the covert rate. Thanks to the developed analytical expressions, we obtain closed-form expressions for the sub-optimal power allocation coefficient for each problem. Simulation results validate the efficacy of the analytical mathematical frameworks and reveal that the proposed approaches of power allocation can provide attractive performance improvement compared to fixed power allocations only.



**Citation:** Doan TB, Nguyen T-H (2025) Enhancing covert communication in NOMA systems with joint security and covert design. PLoS ONE 20(1): e0317289. https://doi.org/10.1371/journal.pone.0317289

**Editor:** Mohammad Reza Ghavidel Aghdam, Ozyegin University: Ozyegin Universitesi, TÜRKIYE

**Received:** November 13, 2024

**Accepted:** December 25, 2024

**Published:** January 13, 2025



**Data Availability Statement:** Data available within the manuscript.

**Funding:** The author(s) received no specific funding for this work.

**Competing interests:** NO authors have competing interests.

## 1 Introduction

### 1.1 Background and motivation

Internet-of-Things (IoT), a new paradigm shift in wireless communication, has recently opened a new chapter for linking billions of devices across domains, where the widespread adoption of IoT devices yields several remarkable improvements in efficiency, automation, and data-driven decision-making. However, this raises critical concerns of security [1], covert communications [2], and reliability [3]. The main reason for these trends mainly stems from the design limitations of IoT devices in terms of computing power, processing power, and resilience, which makes their data transmission vulnerable to malicious attacks, such as

jamming, poisoning, and denial-of-service (DoS) [1]. Especially, due to the simple encryption of communication data, any information transmitted by IoT nodes can be easily captured by eavesdroppers capable of strong processing capability through eavesdropping and monitoring actions. Even if traditional encryption methods can be used to challenge the eavesdropper's decryption, sensitive information can still be revealed by analyzing metadata components, and a prime example of this is network traffic patterns [4]. Another example is in defence scenarios, where communications need to be both secure and covert, ensuring that even the existence of the communication is hidden from adversaries. Since traditional encryption methods fall short of providing this level of protection, transmitting data information over wireless open environments like IoT requires the new development of an efficient security approach aware of the privacy feature.

On the other hand, providing reliable communication and high data rate transmission plays an important role in IoT networking developments. This facilitates IoT nodes with limited hardware to achieve stable connectivity and consistent communication quality in the context of dynamic situations such as channel conditions or fading phenomena. Among potential candidates, non-orthogonal multiple access (NOMA) technology is a promising choice for the next generation of IoT networks [5, 6], for its ability to enable multiple NOMA users to share the same time slots, frequency bands, and spreading codes by taking advantages of user signal superimposed in the power domain and successive-interference cancellation technique to separate the signals [7–9]. Accordingly, NOMA has been investigated in various scenarios of wireless transmissions. For example, in millimeter wave multiple-input multiple-output systems, the work in [10] considered finding the optimal random beamforming coefficients by minimizing the outage probability (OP) for NOMA users. The work in [11] proposed the use of space-time block coding schemes combined with NOMA to reduce communication overhead and latency. In [12], the authors employed random near-far NOMA pairing while optimizing the power allocation and beamforming coefficients to enhance the system performance. Another example of NOMA applications is in limited energy resources. For example, the work in [13] investigated the NOMA for cooperative IoT networks in the presence of co-channel interference. In [14], the authors investigated the functionality of NOMA combined with simultaneously transmitting and reflecting intelligent surface, along with analysis of the performance limits of OP and the tradeoffs between energy and rate as well as between energy and reliability.

NOMA not only delivers fundamental benefits as mentioned above but also helps improve security and covert communication. For example, by dynamically managing power distribution and refining coding and decoding methods, NOMA can help reduce the risks of eavesdropping and illegal entities [15–18]. Especially in cases where a transmitter needs to communicate with a receiver without being detected by a warden, NOMA can leverage background noise in conjunction with inter-user interference (i.e., covert signal is encoded together with public or overt signal) to confuse the surveillance activity, thereby improving covert transmission [19–23].

## 1.2 Literature review

**1.2.1 Reliability aspect.** The popularity of NOMA in improving transmission reliability for IoT networks has been demonstrated in several studies in recent years. For instance, a novel target power allocation (PA) approach for uplink NOMA-based IoT systems was proposed in [24], with an emphasis on the importance of the trade-off between sum rate and reliability in enhancing the overall performance. By generalizing the model proposed in [24] to cellular IoT networks, an adaptive rate NOMA scheme was introduced in [25] to enhance the

IoT user capacity and reduce delay transmissions simultaneously. In [26], NOMA protocols were exploited as a bridge to connect cellular systems with IoT networks, allowing the former to have wide communication coverage to support cell-edge users and the latter to flexibly access licensed spectrum to enhance its quality-of-service. The efficacy of this shared communication protocol was confirmed through the analysis of OP. The benefit of the NOMA protocol in improving reliable communication was demonstrated in wirelessly powered cognitive radio paradigms [27], where the authors show that jointly optimizing user power distribution and energy harvesting time-switching factor can efficiently minimize the OP and maximize the system throughput.

**1.2.2 Secure aspect.** Similar to the reliability aspect, the research on NOMA with physical-layer security has also been explored in many eavesdropper contexts. For example, in [15], a joint power and beamforming design was proposed to deal with the issue of pairing untrusted near users with far users. In [16], the performance quality of terrestrial-integrated aerial IoT NOMA systems with the existence of aerial eavesdroppers was characterized by a secrecy outage probability (SOP) framework. To avoid the outage floor in a secured NOMA system with short-packet transmission, a novel PA strategy was developed in [17], along with analyses of trade-offs in security-efficiency and security-reliability. In [18], the authors analyzed the security performance of short-packet NOMA-IoT networks by deriving a secrecy rate formula.

**1.2.3 Covert aspect.** Several investigations have analyzed the prospect of NOMA in IoT systems from various covert communication perspectives. In [19], a covert NOMA scheme was introduced for cooperative device-to-device communication. This scheme focuses on characterizing the detection error probability (DEP) of the eavesdropper, followed by the finding of the minimal DEP as the worst-case scenario of the main system to lay the foundation for maximizing covert throughput. Inspired by this, the work in [20] proposed to enhance the covert throughput in downlink NOMA IoT systems by optimizing the PA policy under the constraints of the DEP and OP. Similarly, the work in [21] also focused on the same covert maximization problem in [20] but in light of the network's uncertain channel state information. In [22], the authors examined the ergodic rate maximization by optimizing the power resource under the detection threshold constraint. The work in [23] designed a random artificial noise-based beamforming scheme to reduce the eavesdropping rate of the strong user while enhancing the covert communication rate. Very recently, the work in [28] presented a comprehensive analysis and optimization frameworks for the OP, SOP, and DEP performance of active reconfigurable repeater for NOMA systems in the context of IoTs.

Despite the promise of NOMA in providing high-reliability transmission, secured communication services, and advanced covert transmission, very limited studies have explored enhancing covert communication quality in NOMA-based IoT systems through a joint assessment of reliability, security, and confidentiality. For example, the research in [15, 16, 18] provides solid mathematical frameworks for SOP, effective secrecy throughput, and effective secrecy rate but their correlation in enhancing the quality of the system has been not touched yet except for [17]. Similarly, the works in [19–23] mostly study how to derive the mathematical frameworks for the OP, DEP, and effective covert throughput, where only two investigations in [20, 21] take into consideration of both DEP and OP constraints to the covert throughput maximization. Likewise, the work in [28] investigated the analysis and optimization tasks for the OP, SOP, and DEP but in separate manners.

## 1.3 Novelty and contributions

As discussed in Sections 1.1 and 1.2, given the potential nature of NOMA technology, it is apparent that the development of joint secure and confidential communication protocols to

improve reliable transmission in IoT networks has not yet received sufficient attention. Therefore, increasing research efforts in this aspect is timely and necessary. To fill this important gap in the literature, we focus on jamming-assisted covert NOMA systems, where the covert signal of a nearby user is embedded with a public signal of the far user using NOMA transmission and a friendly jammer is deployed to confuse the surveillance of eavesdroppers. In this context, we start with a mathematical framework for evaluating key performance indicators of reliability, security and covertness to comprehensively observe the system characteristics. Then, we provide an optimization framework to enhance the quality of covert transmission in NOMA-based systems. In summary, the main contributions of this work include

1. From the eavesdropper's perspective, we derive the exact DEP expression for the surveillance situation. We then implement the lower-bound optimal DEP by considering the worst-case scenario where the eavesdropper can optimize his judgment threshold. This analysis will serve as an effective guideline for developing a covert communication design of the main system. By assuming that the eavesdropper is able to distinguish the covert signal from the overt signal through monitoring, we further quantify the exact and approximate closed-form expressions for the SOP in the eavesdropping situation.
2. From the users' perspective, we derive closed-form expressions for the covert and public OP as well as ergodic rate formulas. To gain insight into the impact of the transmitted signal-to-noise ratio (SNR) on users' performance, we have also conducted the asymptotic OP and ergodic rate analyses.
3. Building upon both user and eavesdropper behaviors, we formulate and address two problems of optimizing the NOMA power distribution to minimize covert OP and maximize covert ergodic rate under strict requirements of systems, where sub-optimal closed-form expressions for the PA coefficient are derived. By realizing our proposed optimization frameworks, the system can achieve triple goals simultaneously, including reliability, security, and covertness.

Numerical results verify the correctness of the developed mathematical frameworks while demonstrating the proposed optimization frameworks in minimizing covert outage performance and maximizing the covert rate transmission, both following stringent requirements of reliability, security and covertness.

### 1.4 Structure of the paper

The remaining structure of this work can be summarized as follows. We start with the system model description in Section 2, followed by Section 3 with detailed performance analysis, critical problems on providing effective covert communication design, and how to solve these problems. Section 4 provides numerical examples to validate the developed mathematical evaluation and optimization frameworks on the one hand as well as explore the impacts of system parameters on the other hand. Finally, we conclude the paper with Section 5.

## 2 System model description

As depicted in Fig 1, we consider a downlink NOMA system, where source information $\mathsf{S}$ communicates with two users, one covert near user $\mathsf{U}_1$ and one public far user $\mathsf{U}_2$, by NOMA signaling $x_{\text{no}} = \sqrt{\rho}x_2 + \sqrt{(1-\rho)}x_1$ under the surveillance of an eavesdropper $\mathsf{E}$ who can be an idle user or potential eavesdropping candidate. $0.5 < \rho < 1$ is the PA factor while $x_1$ and $x_2$ represent the intended signals of $\mathsf{U}_1$ and $\mathsf{U}_2$, respectively, such that $\mathbb{E}\{|x_1|\} = \mathbb{E}\{|x_2|\} = 0$ and $\mathbb{E}\{|x_1|^2\} = \mathbb{E}\{|x_2|^2\} = 1$. A jammer ($\mathsf{J}$) is deployed to support main channel communication

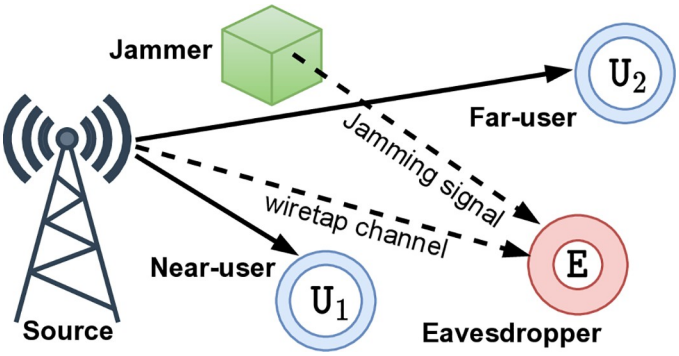


**Fig 1. A downlink NOMA system: One source, one jammer, a pair of NOMA users, and one eavesdropper.**

https://doi.org/10.1371/journal.pone.0317289.g001

by continuously generating artificial noise $x_{ja}$ with power $p_j$ to degrade the quality of E, and $x_{ja}$ is shared for users, with $\mathbb{E}\{|x_{ja}|^2\} = 1$. In this investigation, both $U_1$ and $U_2$ are assumed to know the channel state information (CSI) from S and J to themselves, enabling them to remove the jamming signal detection from the received signal, then subtract this jamming component, and finally decode their information signal. This CSI can be obtained via uplink pilot training while the absence of channel feedback results in S only obtaining the statistical CSI of E. We focus on the scenario E performs two phases of detection and decoding processes to determine whether S transmits a signal to $U_2$ and then goes into decoding $U_2$'s signal if it is detected.

Accordingly, to better enhance its physical layer security performance, let us go into the details of communication characteristics at $U_2$, $U_1$, and E. Denote by $g_{XY}$ is the channel of links from node $X \in \{S, J\}$ to node $Y \in \{U_2, U_1, E\}$, and it follows Rayleigh fading distribution with scale parameter $\Omega_{XY}$. Thus, the Probability Density Functions (PDF) and Cumulative Distribution Functions (CDF) of the channel gain $|g_{XY}|^2$ can be, respectively, modeled as in [9, Eqs. (13) and (14)] as

$$f_{|g_{XY}|^2}(x) = \exp(-x/\Omega_{XY})/\Omega_{XY}, \tag{1}$$

$$F_{|g_{XY}|^2}(x) = 1 - \exp(-x/\Omega_{XY}). \tag{2}$$

Given the transmit power $p_s$ by S, the signal received at Y under the additive white Gaussian noise (AWGN) $n_Y$ can be rewritten as

$$y_Y = \sqrt{p_s} x_{no} g_{SY} + \sqrt{p_j} x_{ja} g_{JY} + n_Y, \; n_Y \sim \mathcal{CN}(0, \sigma^2). \tag{3}$$

Due to a smaller power level allocated, $U_1$ decodes his signal by performing the successive-interference cancellation (SIC) process to subtract the decoded signal $x_2$ from the received signal and then decode $x_1$ under perfect SIC assumption. The achievable rates of decoding $x_2$ and $x_1$ at $U_1$ can be respectively written as

$$C_{U_1}^{x_2} = \log_2\left(1 + \frac{\rho\bar{\gamma}_s|h_{SU_1}|^2}{(1-\rho)\bar{\gamma}_s|h_{SU_1}|^2 + 1}\right), C_{U_1}^{x_1} = \log_2\left(1 + (1-\rho)\bar{\gamma}_s|h_{SU_1}|^2\right), \tag{4}$$

where $\bar{\gamma}_s = p_s/\sigma^2$ presents the average transmit signal-to-noise ratio (SNR). As an unauthorized entity, E has no information regarding $x_1$, and thus, a radiometer is employed with two hypotheses to determine the existence of $x_1$: $h_1$ (true—the existence of $x_1$) and $h_0$ (false—the

none of $x_1$). Thus, the signal observed at E can be classified into

$$y_{\mathsf{E}} = \begin{cases} \sqrt{p_s} x_{\text{no}} h_{\mathsf{SE}} + \sqrt{p_j} g_{\mathsf{JE}} + n_{\mathsf{E}}, & h_1 \\ \sqrt{p_s}\sqrt{\rho} x_2 h_{\mathsf{SE}} + \sqrt{p_j} g_{\mathsf{JE}} + n_{\mathsf{E}}, & h_0 \end{cases} \tag{5}$$

Denote by $d_1$ and $d_0$ the respective decisions of events $h_1$ and $h_0$, and $\zeta$ is the judgment threshold for deciding whether $h_1$ or $h_0$.

Suppose that E is able to successfully detect $x_1$; and thus, the achievable rate of decoding $x_1$ at E can be expressed as

$$C_{\mathsf{E}} = \log_2\left(1 + \frac{(1-\rho)\bar{\gamma}_s |g_{\mathsf{SE}}|^2}{\bar{\gamma}_j |g_{\mathsf{JE}}|^2 + 1}\right). \tag{6}$$

From the aforementioned above, we next turn to explore the performance behaviour of monitoring and eavesdropping activities and then establish an appropriate strategy to enhance the system's covert performance in the following section.

## 3 Performance analysis, problem statement, and solution

This section first analyzes the performance of detecting $x_1$ and intercepting $x_1$ at E, then formulate the strategies to enhance the system performance, and finally provide the corresponding efficient solutions.

### 3.1 Performance analysis

In the context of performance analysis, achieving closed-form expressions in wireless performance analysis helps provide simplified and exact representations of complex relationships, enabling quick and efficient evaluations of performance metrics, and offering deep insights into the system behaviour without extensive simulations. This is because such closed-form expressions can be readily programmable by common package software like Matlab, mathematical, and Maple. As such, one can evaluate specific scenarios of network deployments by replacing input parameters before using them for online implementations. Therefore, in this study, we will analyze the system performance by first deriving closed-form expressions for the DEP, SOP, OP, and rate metrics.

**3.1.1 Monitoring analysis.** To have the best knowledge on the behaviour of monitoring $x_1$ at E for improving the security transmission at the physical layer, this subsection will analyze the DEP in the role of an eavesdropper. This is because the DEP metric will reflect the level of error probability that the eavesdropper encounters during the monitoring process. To be specific, we first derive the DEP by assuming the judgment threshold is fixed, i.e., $\zeta$. Based on this, we then quantify how the eavesdropper will optimize the judgment threshold $\zeta$ to minimize the DEP metric. Such analysis would provide useful benchmarks in enhancing security countermeasures since it focuses on the worst-case scenario, where DEP is minimized at an eavesdropper.

In detail, we first go into deriving the exact DEP, which can be mathematically written as

$$\text{DEP}_{\mathsf{E}} = \Pr[d_1|h_0] + \Pr[d_0|h_1], \tag{7}$$

where the first probability implies that the transmission of $x_1$ observed by E exists but there is no actual transmission. In contrast, the second probability refers to no transmission observed by E, but there is a transmission of $x_1$.

Similar to [19–23], we assume that the infinite number of signal examples are collected by $\mathsf{E}$ to detect $x_2$. Thus, the first probability in (7) can be derived from (5) as

$$\begin{aligned}\Pr[d_1|\mathcal{H}_0] &= \Pr[p_s\rho|h_{\mathsf{SE}}|^2 + p_j|h_{\mathsf{JE}}|^2 + \sigma^2 \geq \zeta] = 1 - \Pr[\bar{\gamma}_s\rho|h_{\mathsf{SE}}|^2 \leq \Delta - \bar{\gamma}_j|h_{\mathsf{JE}}|^2] \\ &= 1 - \int_0^{\frac{\Delta}{\bar{\gamma}_j}} F_{|h_{\mathsf{SE}}|^2}\left(\frac{\Delta - \bar{\gamma}_j x}{\bar{\gamma}_s\rho}\right) f_{|h_{\mathsf{JE}}|^2}(x)dx \\ &= 1 - F_{|h_{\mathsf{JE}}|^2}\left(\frac{\Delta}{\bar{\gamma}_j}\right) + \int_0^{\Delta/\bar{\gamma}_j} \exp\left(-\frac{x}{\Omega_{\mathsf{JE}}}\right)\frac{1}{\Omega_{\mathsf{JE}}}\exp\left(-\frac{\Delta - \bar{\gamma}_j x}{\bar{\gamma}_s\rho\Omega_{\mathsf{SE}}}\right)dx \\ &= 1 - F_{|h_{\mathsf{JE}}|^2}\left(\frac{\Delta}{\bar{\gamma}_j}\right) + \frac{\bar{\gamma}_s\rho\Omega_{\mathsf{SE}}}{\bar{\gamma}_s\rho\Omega_{\mathsf{SE}} - \bar{\gamma}_j\Omega_{\mathsf{JE}}}\left[\exp\left(-\frac{\Delta}{\bar{\gamma}_s\rho\Omega_{\mathsf{SE}}}\right) - \exp\left(-\frac{\Delta}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right)\right].\end{aligned} \tag{8}$$

where $\bar{\gamma}_j = p_j/\sigma^2$ is the jammer SNR and $\Delta = \zeta/\sigma^2 - 1$. Meanwhile, the second probability in (7) can be derived as

$$\begin{aligned}\Pr[d_0|\mathcal{H}_1] &= \Pr[p_s|h_{\mathsf{SE}}|^2 + p_j|h_{\mathsf{JE}}|^2 + \sigma^2 \leq \zeta] \\ &= F_{|h_{\mathsf{JE}}|^2}(\Delta/\bar{\gamma}_j) - \frac{\bar{\gamma}_s\Omega_{\mathsf{SE}}}{\bar{\gamma}_s\Omega_{\mathsf{SE}} - \bar{\gamma}_j\Omega_{\mathsf{JE}}}\left[\exp\left(-\frac{\Delta}{\bar{\gamma}_s\Omega_{\mathsf{SE}}}\right) - \exp\left(-\frac{\Delta}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right)\right].\end{aligned} \tag{9}$$

By plugging (8) and (9) into (7), we get the following theorem.

**Lemma 1**. The closed-form expression for the DEP of $\mathsf{E}$ can be derived as

$$\mathrm{DEP}_{\mathsf{E}} = 1 + \frac{\exp\left(-\frac{\Delta}{\bar{\gamma}_s\rho\Omega_{\mathsf{SE}}}\right)}{1 - \frac{\bar{\gamma}_j\Omega_{\mathsf{JE}}}{\bar{\gamma}_s\rho\Omega_{\mathsf{SE}}}} - \frac{\exp\left(-\frac{\Delta}{\bar{\gamma}_s\Omega_{\mathsf{SE}}}\right)}{1 - \frac{\bar{\gamma}_j\Omega_{\mathsf{JE}}}{\bar{\gamma}_s\Omega_{\mathsf{SE}}}} + \frac{1}{1 - \frac{\bar{\gamma}_j\Omega_{\mathsf{JE}}}{\bar{\gamma}_s\Omega_{\mathsf{SE}}}}\frac{(1-\rho)}{1 - \frac{\rho\bar{\gamma}_s\Omega_{\mathsf{SE}}}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}}\exp\left(-\frac{\Delta}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right). \tag{10}$$

The result in (10) shows that $\sigma^2$, $\Omega_{\mathsf{SE}}$, $\zeta$, and $\Omega_{\mathsf{JE}}$ are arbitrary values without controlling ability. Meanwhile, examining $\bar{\gamma}_s$ and $\bar{\gamma}_j$ discloses that when $\bar{\gamma}_s, \bar{\gamma}_j \to \infty$ occurs, the DEP $\mathrm{DEP}_{\mathsf{E}}^{\star}$ at $\mathsf{E}$ becomes unity, i.e., $\mathrm{DEP}_{\mathsf{E}} \to 1$. This means that $\mathrm{DEP}_{\mathsf{E}}$ is an increasing function of $\bar{\gamma}_s, \bar{\gamma}_j \to \infty$. However, this is only correct when $\mathsf{E}$ does not optimize its judgement threshold $\zeta$. Therefore, deriving the optimal DEP at $\mathsf{E}$ with the optimization of $\zeta^{\star}$ is necessary but not easy, which motivates us to introduce the following lower-bound optimal DEP.

**Proposition 1**. The lower-bound optimal DEP at $\mathsf{E}$ can be derived as

$$\widetilde{\mathrm{DEP}}_{\mathsf{E}}^{\star} = \rho^{\frac{1}{(1-\rho)}} + 1 - \rho^{\frac{\rho}{(1-\rho)}}. \tag{11}$$

*Proof*. Let us reconsider the probabilities in (7) by conditioning on $X = |h_{\mathsf{JE}}|^2$ as

$$\Pr[d_1|\mathcal{H}_0|X] = 1 - \Pr\left[p_s\rho|h_{\mathsf{SE}}|^2 \leq \zeta - p_jX - \sigma^2\right] = \exp\left(-\frac{\Delta - \bar{\gamma}_jX}{\Omega_{\mathsf{SE}}\bar{\gamma}_s\rho}\right), \tag{12}$$

$$\Pr[d_0|\mathcal{H}_1|X] = \Pr\left[p_s|h_{\mathsf{SE}}|^2 + p_jX + \sigma^2 \leq \zeta|\right] = 1 - \exp\left(-\frac{\Delta - \bar{\gamma}_jX}{\Omega_{\mathsf{SE}}\bar{\gamma}_s}\right). \tag{13}$$

By plugging (12) and (13) into (7) and then taking Δ with respect to ζ equal zero, we get that

$$\begin{aligned}\frac{\partial \mathrm{DEP}_{\mathsf{E}}}{\partial \Delta} &= -\frac{1}{\Omega_{\mathsf{SE}}\bar{\gamma}_s\rho}\exp\left(-\frac{\Delta-\bar{\gamma}_j X}{\Omega_{\mathsf{SE}}\bar{\gamma}_s\rho}\right)+\frac{1}{\Omega_{\mathsf{SE}}\bar{\gamma}_s}\exp\left(-\frac{\Delta-\bar{\gamma}_j X}{\Omega_{\mathsf{SE}}\bar{\gamma}_s}\right)=0\\ \Rightarrow\ & \frac{1}{\rho}\exp\left(-\frac{\Delta-\bar{\gamma}_j X}{\Omega_{\mathsf{SE}}\bar{\gamma}_s\rho}\right)=\exp\left(-\frac{\Delta-\bar{\gamma}_j X}{\Omega_{\mathsf{SE}}\bar{\gamma}_s}\right)\\ \Rightarrow\ & \ln\left(\frac{1}{\rho}\right)-\frac{\Delta-\bar{\gamma}_j X}{\Omega_{\mathsf{SE}}\bar{\gamma}_s\rho}=\frac{\bar{\gamma}_j X-\Delta}{\Omega_{\mathsf{SE}}\bar{\gamma}_s}\\ \Rightarrow\ & \frac{\Omega_{\mathsf{SE}}\bar{\gamma}_s\rho}{(1-\rho)}\ln\left(\frac{1}{\rho}\right)+\bar{\gamma}_j X=\Delta.\end{aligned} \tag{14}$$

Finally, plugging Δ in (12) and (13), we get the lower-bound optimal DEP.

**Remark 1**. The result in (11) reveals that $\widetilde{\mathrm{DEP}}^{\star}_{\mathsf{E}}$ is increased with an increase in $\rho$. Specifically, when $\rho = 0$, we get $\widetilde{\mathrm{DEP}}^{\star}_{\mathsf{E}} = 0$. When $\rho = 0.5$, $\widetilde{\mathrm{DEP}}^{\star}_{\mathsf{E}} = 1 + 0.5^{1/0.5} - 0.5^{1} = 0.75$. When $\rho \to 1$, $\widetilde{\mathrm{DEP}}^{\star}_{\mathsf{E}} \to 1$ since $\lim_{\rho\to 1}\rho^{1/(1-\rho)} = 1/\exp(1)$ and $\lim_{\rho\to 1}\rho^{\rho/(1-\rho)} = 1/\exp(1)$, which is attained based on the property of the exponential function limit. On the other hand, it is worth noting that the result (11) will converge to the exact optimal DEP at $\mathsf{E}$ whenever $\bar{\gamma}_j \leq \bar{\gamma}_s$, which shall be soon demonstrated in numerical results.

**3.1.2 Analysis of eavesdropping activity.** In this section, we will further go into a detailed analysis of the case where the eavesdropper can detect the covert signal from the monitoring activity and then try to wiretap this signal. Herein, we focus on evaluating the SOP performance as the role of the legitimate system rather than the eavesdropper in the previous section. Specifically, the SOP metric will reflect how much probability that the legitimate link's channel capacity $C_{\mathsf{E}}$ is larger than the eavesdropper link's channel capacity $C^{x_1}_{\mathsf{U}_1}$ when compared to a given secrecy rate $R_1$ of decoding design, i.e., $C^{x_1}_{s} = [C^{x_1}_{\mathsf{U}_1} - C_{\mathsf{E}}] < R_1$. If $C^{x_1}_{\mathsf{U}_1} - C_{\mathsf{E}}$ is negative and its magnitude is larger than the secure rate $R_1$, it means that the eavesdropper can strongly wiretap the covert signal with the probability of one. This means that using security techniques like encryption is not effective. Conversely, $C^{x_1}_{\mathsf{U}_1} - C_{\mathsf{E}}$ is positive. This means that the eavesdropper can have a quality of achievable rate worse than the legitimate user, and if this achieved rate gap is larger than the secure rate, the eavesdropper cannot decode any information. In other words, using security techniques is entirely effective.

Following that, the SOP that $\mathsf{E}$ eavesdrops on $x_1$ can be mathematically written as follows:

$$\mathrm{SOP}_{\mathsf{E}} = \Pr(C^{x_1}_{\mathsf{U}_1} - C_{\mathsf{E}} < R_1). \tag{15}$$

By substituting (4) and (6) into (15), the SOP that E eavesdrops on $x_1$ can be derived as

$$\begin{aligned}
\mathrm{SOP}_{\mathsf{E}} &= \Pr\left(\frac{1+(1-\rho)\bar{\gamma}_s|g_{\mathsf{SU}_1}|^2}{1+\frac{(1-\rho)\bar{\gamma}_s|g_{\mathsf{SE}}|^2}{Y}} < \tau|Y \triangleq \bar{\gamma}_j|g_{\mathsf{JE}}|^2+1\right)\\
&= \int_0^{\infty} F_{|g_{\mathsf{SU}_1}|^2}\left(\frac{\phi+\tau(1-\rho)\bar{\gamma}_s x/Y}{(1-\rho)\bar{\gamma}_s}\right) f_{|g_{\mathsf{SE}}|^2}(x)dx\\
&= 1-\exp\left(-\frac{\phi/\Omega_{\mathsf{SU}_1}}{(1-\rho)\bar{\gamma}_s}\right)\int_1^{\infty}\frac{y f_Y(y)dy}{y+\tau\Omega_{\mathsf{SE}}/\Omega_{\mathsf{SU}_1}}\\
&= 1-\exp\left(-\frac{\phi}{(1-\rho)\bar{\gamma}_s\Omega_{\mathsf{SU}_1}}+\frac{1}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right)\int_1^{\infty}\frac{y\exp\left(-\frac{x}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right)}{y+\tau\Omega_{\mathsf{SE}}/\Omega_{\mathsf{SU}_1}}\frac{1}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}dx\\
&= 1-\exp\left(-\frac{\phi}{(1-\rho)\bar{\gamma}_s\Omega_{\mathsf{SU}_1}}+\frac{1}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right)\frac{1}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\\
&\quad\times\int_1^{\infty}\left[1-\frac{\tau\Omega_{\mathsf{SE}}/\Omega_{\mathsf{SU}_1}}{y+\tau\Omega_{\mathsf{SE}}/\Omega_{\mathsf{SU}_1}}\right]\exp\left(-\frac{x}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right)dx,
\end{aligned} \tag{16}$$

where $\phi = 2^{R_1}-1$. Making use of [29, eq. (3.352.2)], we achieve the following lemma.

**Lemma 2**. Exact closed-form expressions for the SOP that E eavesdrops on $x_1$ can be derived as

$$\mathrm{SOP}_{\mathsf{E}} = 1-\exp(-\phi/[(1-\rho)\bar{\gamma}_s\Omega_{\mathsf{SU}_1}])\Xi, \tag{17}$$

where Ξ is the short-notation of

$$\Xi = 1+\frac{\tau\Omega_{\mathsf{SE}}}{\Omega_{\mathsf{SU}_1}\bar{\gamma}_j\Omega_{\mathsf{JE}}}\exp\left(-\frac{1}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}+\frac{\tau\Omega_{\mathsf{SE}}}{\Omega_{\mathsf{SU}_1}\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right)\mathrm{Ei}\left(-\frac{1}{\bar{\gamma}_j\Omega_{\mathsf{JE}}}-\frac{\tau\Omega_{\mathsf{SE}}}{\Omega_{\mathsf{SU}_1}\bar{\gamma}_j\Omega_{\mathsf{JE}}}\right), \tag{18}$$

where Ei(·) is the exponential integral function [29, Eq. (8.211.1)]. This function is special in mathematics and is defined as the integral of the ratio between an exponential function and its argument. For real non-zero values of (*x*), the exponential integral is given by:

$$\mathrm{Ei}(x) = -\int_{-x}^{\infty}\frac{e^{-t}}{t}dt = \int_{-\infty}^{x}\frac{e^{t}}{t}dt. \tag{19}$$

**Remark 2**. As high SNR, i.e., $\bar{\gamma}_s \to \infty$, the SOP of $\mathsf{U}_1$ in (17) can be upper bounded using the connection $1-\exp(-x) \simeq x$ as $x \to 0$ to get that

$$\widetilde{\mathrm{SOP}}_{\mathsf{E}} = 1-(1-\phi/[(1-\rho)\bar{\gamma}_s\Omega_{\mathsf{SU}_1}])\Xi. \tag{20}$$

**Remark 3**. The result in (20) reveals that the SOP at E is an increasing function of $\rho$ since $\exp(-1/(1-\rho)) \to 0$. When $\bar{\gamma}_s \to \infty$, the SOP at E becomes $\mathrm{SOP}_{\mathsf{E}} \simeq \Xi$ (a constant value).

**3.1.3 Analysis of legitimate user.** This part evaluates the performance of $\mathsf{U}_1$ by deriving the OP and ergodic rate metric. Herein, the OP metric will reflect how much reliable communication users can achieve with the given predefined threshold rate, respectively. Meanwhile, the ergodic rate will clarify how much the average achievable rate that users can obtain when the system uses channel coding/modulation schemes to achieve near-zero errors during signal transmission.

**OP analysis for $\mathsf{U}_1$**: Let $r_i$ is the given predefined threshold rate to decode $x_i$, with $i = 1, 2$. Denoting $\kappa_i = 2^{r_i} - 1$, the OP of decoding $x_1$ at $\mathsf{U}_1$ can be mathematically defined as

$$\mathrm{OP}_{\mathsf{U}_1} = 1 - \Pr[C_{\mathsf{U}_1}^{x_2} > r_2, C_{\mathsf{U}_1}^{x_1} > r_1]. \tag{21}$$

This probability describes all the events that the achievable rates received by $\mathsf{U}_1$ for decoding $x_1$ or $x_2$ or both of them are much less than the required target rates. This means that $\mathsf{U}_1$ cannot decode either $x_1$ or $x_2$ or both of them.

By injecting the formulas of $C_{\mathsf{U}_1}^{x_2}$ and $C_{\mathsf{U}_1}^{x_1}$ in (4) into the above probability, we can rewrite the term $\mathrm{OP}_{\mathsf{U}_1}$ as

$$\begin{aligned} \mathrm{OP}_{\mathsf{U}_1} &= 1 - \Pr\left[|g_{\mathsf{SU}_1}|^2 > \frac{\kappa_2}{\bar{\gamma}_s \psi}, |g_{\mathsf{SU}_1}|^2 > \frac{\kappa_1}{\bar{\gamma}_s(1-\rho)}\right] \\ &= F_{|g_{\mathsf{SU}_1}|^2}\left(\frac{1}{\bar{\gamma}_s}\max\left\{\frac{\kappa_2}{\psi}, \frac{\kappa_1}{(1-\rho)}\right\}\right), \end{aligned} \tag{22}$$

where $\psi = \rho - (1-\rho)\kappa_2 > 0$. Herein, if $\psi \leq 0$, $\mathrm{OP}_{\mathsf{U}_1} = 1$.

By mapping the CDF in (1) with the above result, we obtain the final OP expression for $\mathsf{U}_1$ as

$$\mathrm{OP}_{\mathsf{U}_1} = \begin{cases} 1 - \exp\left(-\dfrac{\max\left\{\frac{\kappa_2}{\psi}, \frac{\kappa_1}{(1-\rho)}\right\}}{\bar{\gamma}_s \Omega_{\mathsf{SU}_1}}\right), & \psi < 0, \\ 1, & \psi \leq 0. \end{cases} \tag{23}$$

**Remark 4**. The result in (23) shows that when $\kappa_2/\psi \geq \kappa_1/(1-\rho)$, the effective region of $\rho$ is

$$\rho \leq \kappa_2(1+\kappa_1)/(\kappa_1(1+\kappa_2)+\kappa_2) \triangleq \varpi. \tag{24}$$

As for this case, increasing $\rho$ decreases $\mathrm{OP}_{\mathsf{U}_1}$. Conversely, increasing $\rho$ gives rise to $\mathrm{OP}_{\mathsf{U}_1}$.

**Remark 5**. At high SNR, i.e., $\bar{\gamma}_s \to \infty$, the OP of $\mathsf{U}_1$ in (23) can be upper bounded as

$$\widetilde{\mathrm{OP}_{\mathsf{U}_1}} \approx \max\{\kappa_2/(\rho - (1-\rho)\kappa_2), \kappa_1(/1-\rho)\}/[\bar{\gamma}_s \Omega_{\mathsf{SU}_1}]. \tag{25}$$

It is clear that $\widetilde{\mathrm{OP}_{\mathsf{U}_1}}$ is proportional to $1/\bar{\gamma}_s$; thus, we can infer that $\mathsf{U}_1$'s diversity order is 1.

**Covert rate analysis for $\mathsf{U}_1$**: The covert rate of sending $x_1$ from $\mathsf{S}$ to $\mathsf{U}_1$ under no error decoding of $x_1$ can be defined as

$$\mathcal{R}_{\mathsf{U}_1} = \mathbb{E}\{\log_2(1 + (1-\rho)\bar{\gamma}_s |h_{\mathsf{SU}_1}|^2)\}. \tag{26}$$

By applying integral by part methods [13, Eq. (30)] and mapping the CDF in (1), we can rewrite the term $\mathcal{R}_{\mathsf{U}_1}$ as

$$\begin{aligned} \mathcal{R}_{\mathsf{U}_1} &= \frac{1}{\ln(2)} \int_0^\infty \frac{1}{1+x}\left[1 - F_{|h_{\mathsf{SU}_1}|^2}\left(\frac{x/\bar{\gamma}_s}{(1-\rho)}\right)\right] dx \\ &= \int_0^\infty \frac{\exp(-x/[\Omega_{\mathsf{SU}_1}(1-\rho)\bar{\gamma}_s])}{\ln(2)(1+x)} dx. \end{aligned} \tag{27}$$

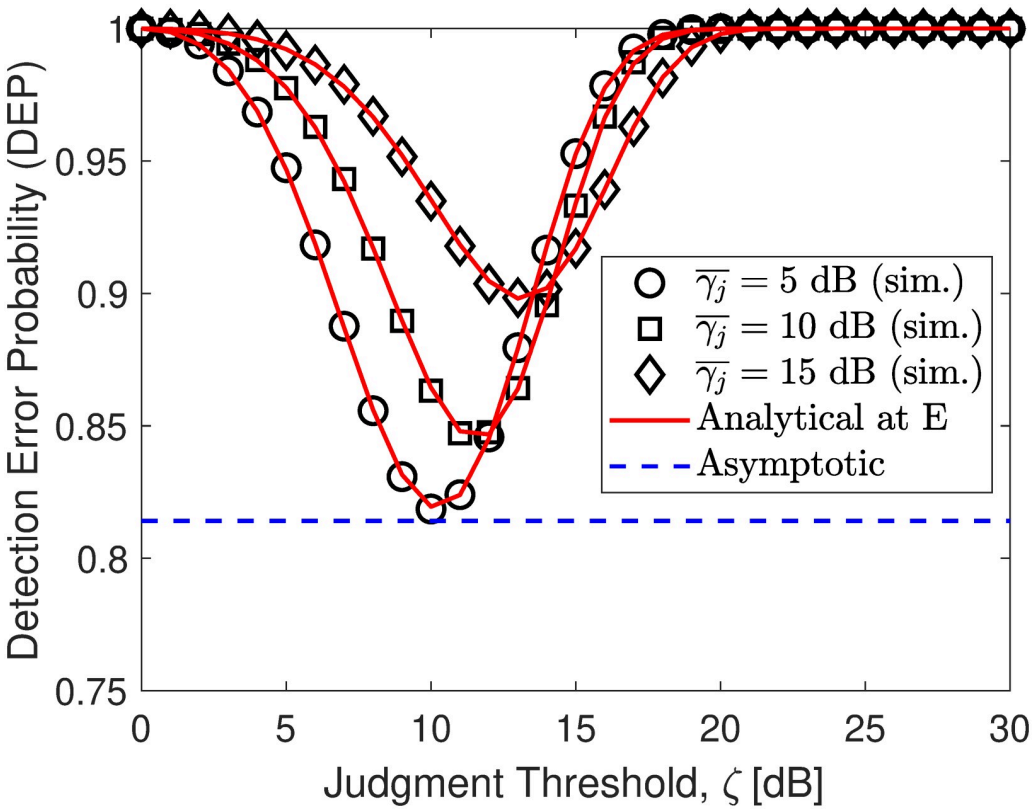


**Fig 2. Impact of $\bar{\gamma}_j$ (jamming SNR) on DEP performance.** Setups: a) $\rho = 0.6$ and $\bar{\gamma}_s = 10$ dB, b) $\bar{\gamma}_j = 5$ dB and $\bar{\gamma}_s = 10$ dB, and c) $\rho = 0.6$ and $\bar{\gamma}_j = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g002

Now, applying the standard form in [29, Eq. (3.352.4)], we get the final expression for the covert rate of sending $x_1$ from S to $\mathsf{U}_1$ as

$$\mathcal{R}_{\mathsf{U}_1} = -\frac{\exp\left(\frac{1/(1-\rho)}{\Omega_{\mathsf{SU}_1}\bar{\gamma}_s}\right)}{\ln(2)}\mathrm{Ei}\left(-\frac{1/(1-\rho)}{\Omega_{\mathsf{SU}_1}\bar{\gamma}_s}\right). \tag{28}$$

**Remark 6**. At high SNR, i.e., $\bar{\gamma}_s \to \infty$, the covert rate of $\mathsf{U}_1$ in (26) can be upper bounded as

$$\widetilde{\mathcal{R}_{\mathsf{U}_1}} \approx \mathbb{E}\{\log_2((1-\rho)\bar{\gamma}_s|h_{\mathsf{SU}_1}|^2)\} = \log_2((1-\rho)\bar{\gamma}_s) + \mathbb{E}\{\log_2(|h_{\mathsf{SU}_1}|^2)\}. \tag{29}$$

Since $\widetilde{\mathcal{R}_{\mathsf{U}_1}}$ scales up with a logarithm function of $\bar{\gamma}_s$, $\mathsf{U}_1$'s multiplexing gain is 1. Besides, we can also observe that $\widetilde{\mathcal{R}_{\mathsf{U}_1}}$ scales down with an increase in $\rho$.

**OP analysis for $\mathsf{U}_2$**: Besides investigating the performance of $\mathsf{U}_1$, it is also necessary to study the performance of serving $\mathsf{U}_2$. Specifically, the OP of $\mathsf{U}_2$ to directly decode its message $x_2$ can be described as

$$\mathrm{OP}_{\mathsf{U}_2} = \Pr[C_{\mathsf{U}_2}^{x_2} < r_2], \tag{30}$$

where $C_{\mathsf{U}_2}^{x_2}$ can be derived similar to $C_{\mathsf{U}_1}^{x_2}$ in (4) by simply replacing $|g_{\mathsf{SU}_1}|^2$ with $|g_{\mathsf{SU}_2}|^2$.

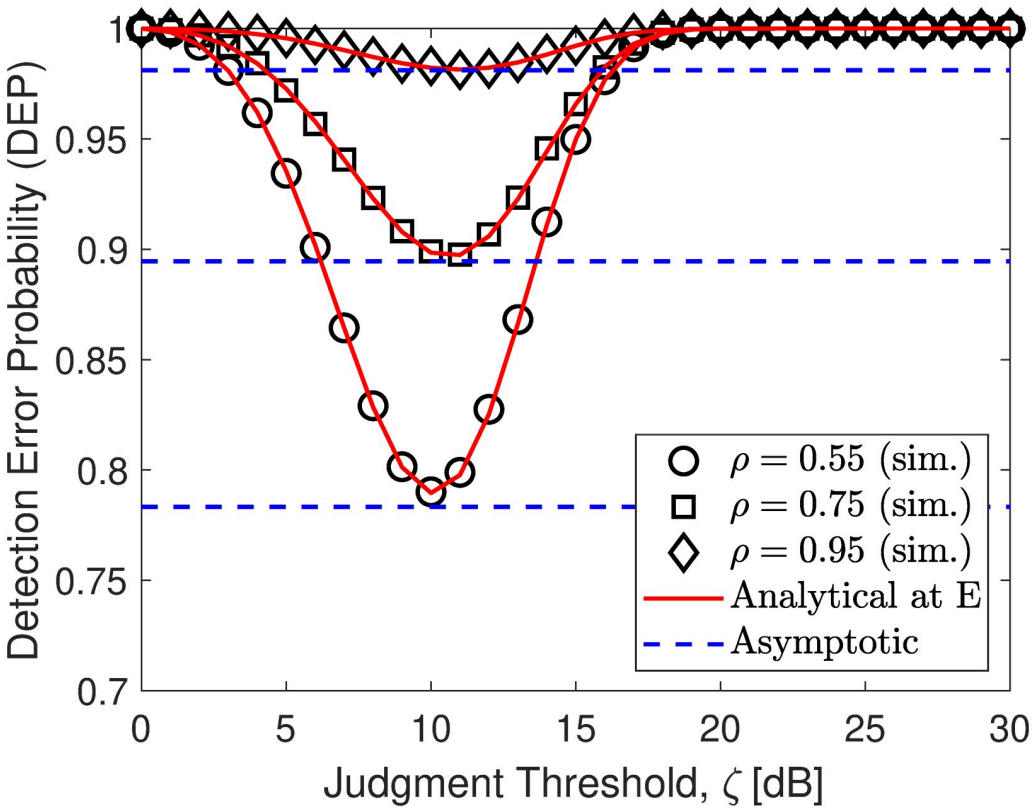


**Fig 3. Impact of $\rho$ (PA coefficient of $\mathsf{U}_2$) on DEP performance.** Setups: a) $\rho$ = 0.6 and $\bar{\gamma}_s = 10$ dB, b) $\bar{\gamma}_j = 5$ dB and $\bar{\gamma}_s = 10$ dB, and c) $\rho$ = 0.6 and $\bar{\gamma}_j = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g003

Accordingly, the OP of $\mathsf{U}_2$ can be derived by mapping with the CDF in (1) as

$$\begin{aligned} \mathrm{OP}_{\mathsf{U}_2} &= \Pr\left(|g_{\mathsf{SU}_2}|^2 < \frac{\kappa_2}{\bar{\gamma}_s \psi}\right) = F_{|g_{\mathsf{SU}_2}|^2}\left(\frac{\kappa_2}{\bar{\gamma}_s \psi}\right) \\ &= 1 - \exp\left(-\frac{\kappa_2/[\Omega_{\mathsf{SU}_2}\bar{\gamma}_s]}{(\rho(1+\kappa_2)-\kappa_2)}\right). \end{aligned} \tag{31}$$

**Remark 7**. Directly inspection of (31) shows that increasing $\bar{\gamma}_s$, $\rho$ or decreasing $\kappa_2$ will decrease $\mathrm{OP}_{\mathsf{U}_2}$, i.e., improving the outage event to the smallest possible extent.

**Remark 8**. At high SNR, i.e., $\bar{\gamma}_s \to \infty$, the OP of $\mathsf{U}_2$ can be upper bounded as

$$\widetilde{\mathrm{OP}_{\mathsf{U}_2}} \approx \kappa_2/[\bar{\gamma}_s \Omega_{\mathsf{SU}_1}(\rho - (1-\rho)\kappa_2)] = \kappa_2/[\bar{\gamma}_s \Omega_{\mathsf{SU}_1}(\rho(1+\kappa_2) - \kappa_2)]. \tag{32}$$

Since $\widetilde{\mathrm{OP}_{\mathsf{U}_2}}$ is proportional to $1/\bar{\gamma}_s$, $\mathsf{U}_2$'s diversity gain is 1.

**Covert rate analysis for $\mathsf{U}_2$**: The public rate of sending $x_2$ from $\mathsf{S}$ to $\mathsf{U}_2$ can be defined as

$$\mathcal{R}_{\mathsf{U}_2} = \mathbb{E}\left\{\log_2\left(1 + \frac{\rho\bar{\gamma}_s|g_{\mathsf{SU}_2}|^2}{(1-\rho)\bar{\gamma}_s|g_{\mathsf{SU}_2}|^2 + 1}\right)\right\}, \tag{33}$$

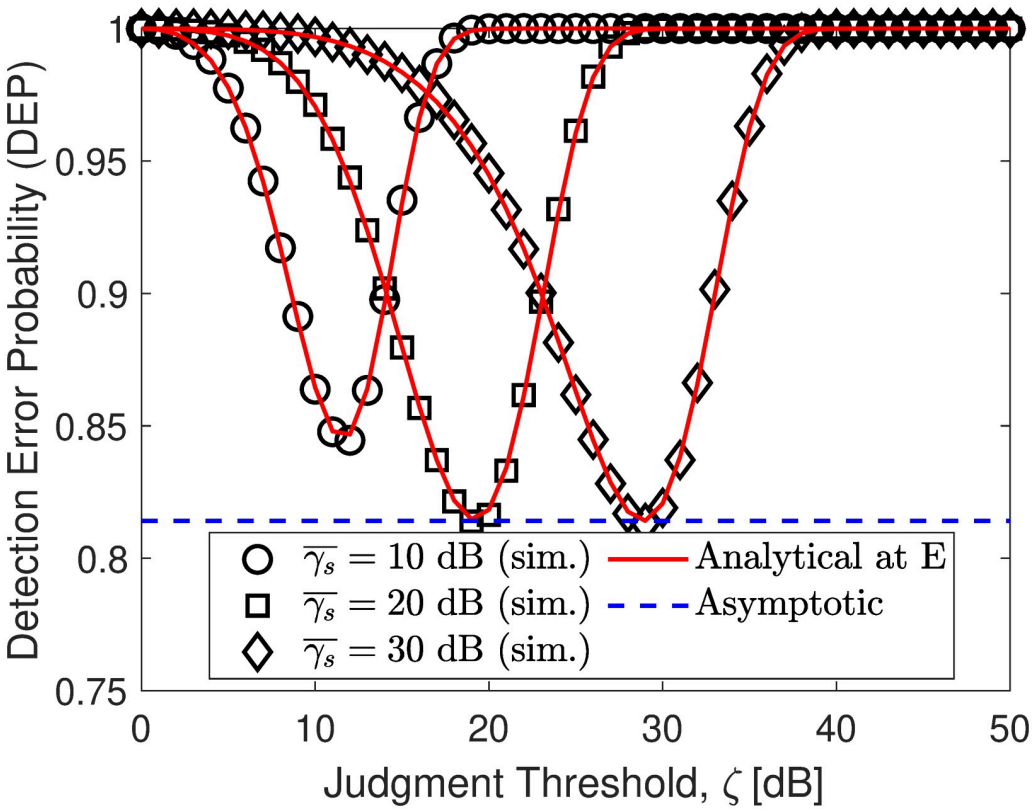


**Fig 4. Impact of $\bar{\gamma}_s$ (transmit SNR) on DEP performance.** Setups: a) $\rho = 0.6$ and $\bar{\gamma}_s = 10$ dB, b) $\bar{\gamma}_j = 5$ dB and $\bar{\gamma}_s = 10$ dB, and c) $\rho = 0.6$ and $\bar{\gamma}_j = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g004

To solve the above expression, we first apply the logarithm decomposition and then apply the integral by part methods as

$$\begin{aligned}\mathcal{R}_{\mathsf{U}_2} &= \mathbb{E}\{\log_2(1+\bar{\gamma}_s|g_{\mathsf{SU}_2}|^2)\} - \mathbb{E}\{\log_2(1+(1-\rho)\bar{\gamma}_s|g_{\mathsf{SU}_2}|^2)\} \\ &= \frac{1}{\ln(2)}\int_0^\infty \frac{1-F_{|h_{\mathsf{SU}_2}|^2}\left(\frac{x}{\bar{\gamma}_s}\right)}{1+x}dx - \frac{1}{\ln(2)}\int_0^\infty \frac{1-F_{|h_{\mathsf{SU}_2}|^2}\left(\frac{x}{(1-\rho)\bar{\gamma}_s}\right)}{1+x}dx.\end{aligned} \tag{34}$$

Now, using the standard form in [29, Eq. (3.352.4)], we get the final expression for the public rate of sending $x_2$ from $\mathsf{S}$ to $\mathsf{U}_2$ as

$$\mathcal{R}_{\mathsf{U}_2} = \frac{\mathrm{Ei}(-1/[(1-\rho)\Omega_{\mathsf{SU}_2}\bar{\gamma}_s])}{\ln(2)\exp(-1/[(1-\rho)\Omega_{\mathsf{SU}_2}\bar{\gamma}_s])} - \frac{\mathrm{Ei}(-1/[\Omega_{\mathsf{SU}_2}\bar{\gamma}_s])}{\ln(2)\exp(-1/[\Omega_{\mathsf{SU}_2}\bar{\gamma}_s])}. \tag{35}$$

**Remark 9**. At high SNR, i.e., $\bar{\gamma}_s \to \infty$, the public rate of $\mathsf{U}_2$ can be upper bounded as

$$\widetilde{\mathcal{R}_{\mathsf{U}_2}} \approx \mathbb{E}\{\log_2(\bar{\gamma}_s|g_{\mathsf{SU}_2}|^2)\} - \mathbb{E}\{\log_2((1-\rho)\bar{\gamma}_s|g_{\mathsf{SU}_2}|^2)\} = -\log_2(1-\rho). \tag{36}$$

Since $\widetilde{\mathcal{R}_{\mathsf{U}_2}}$ does not scale up with a logarithm function of $\bar{\gamma}_s$, $\mathsf{U}_2$'s multiplexing gain is 0. Besides, we can also observe that $\widetilde{\mathcal{R}_{\mathsf{U}_1}}$ scales up with an increase in $\rho$.

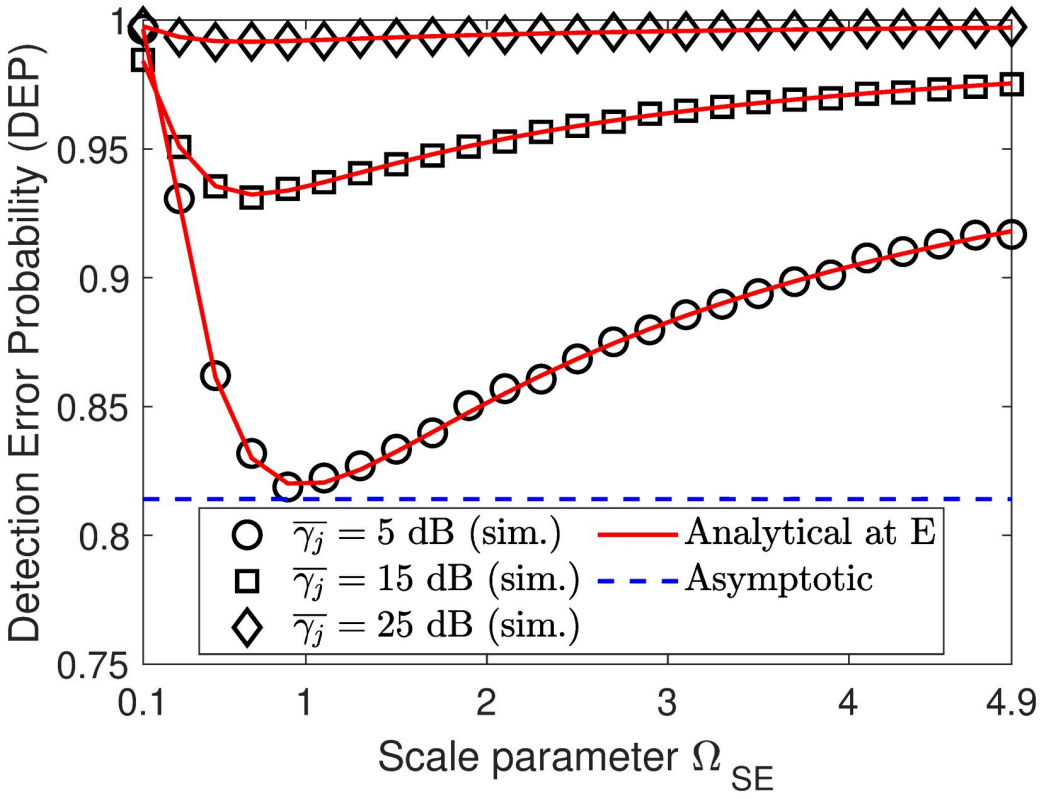


**Fig 5. Impact of fading parameter $\Omega_{SE}$ on DEP performance.** Setups: $\rho = 0.6$, $\overline{\gamma}_s = 10$ dB, and $\zeta = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g005

### 3.2 Outage performance optimization

Having all the expressions of the lower-bound optimal DEP, the SOP, and the OP metrics in hand, in this section, we will first formulate the problem of optimizing resource power allocation subject to minimize the reliability of sending covert information while ensuring reliable communication of public signal at all legitimate users (passing SIC process at $\mathsf{U}_1$ and successfully decoding at $\mathsf{U}_2$) as well as two lines of security countermeasures for the physical layer transmission (one line from the monitoring signal of covert signals and another line for decoding covert information). Afterward, we will provide detailed guidance in achieving closed-form sub-optimal PA policy.

**3.2.1 Problem formulation.** In this subsection, we seek an efficient approach to ensure the covert transmission is not disclosed by an unauthorized thirsty party $\mathsf{E}$ while ensuring reliable communication for all users. To be specific, we aim to improve the covert transmission of $\mathsf{U}_1$ in terms of OP by optimizing the PA coefficient $\rho$ while ensuring the maximum eavesdropping $\epsilon_{\mathsf{E}}$, the minimum covertness $\varrho_{\mathsf{U}_2}$, and the minimum OP $\varepsilon_{\mathsf{U}_2}$. Mathematically, this optimization problem can be formulated as

$$\min_{\rho} \ \mathrm{OP}_{\mathsf{U}_1} \tag{37a}$$

$$\text{s.t} \ \ \mathrm{OP}_{\mathsf{U}_2} \leq \varepsilon_{\mathsf{U}_2}, \mathrm{SOP}_{\mathsf{E}} \leq \epsilon_{\mathsf{E}}, \mathrm{DEP}^{\star}_{\mathsf{E}} \geq \varrho_{\mathsf{U}_2}, \tag{37b}$$

$$\rho \geq \kappa_2/(1+\kappa_2) + \ell, 1 - \ell \geq \rho \geq 0.5 + \ell, \ell \simeq 0, \tag{37c}$$

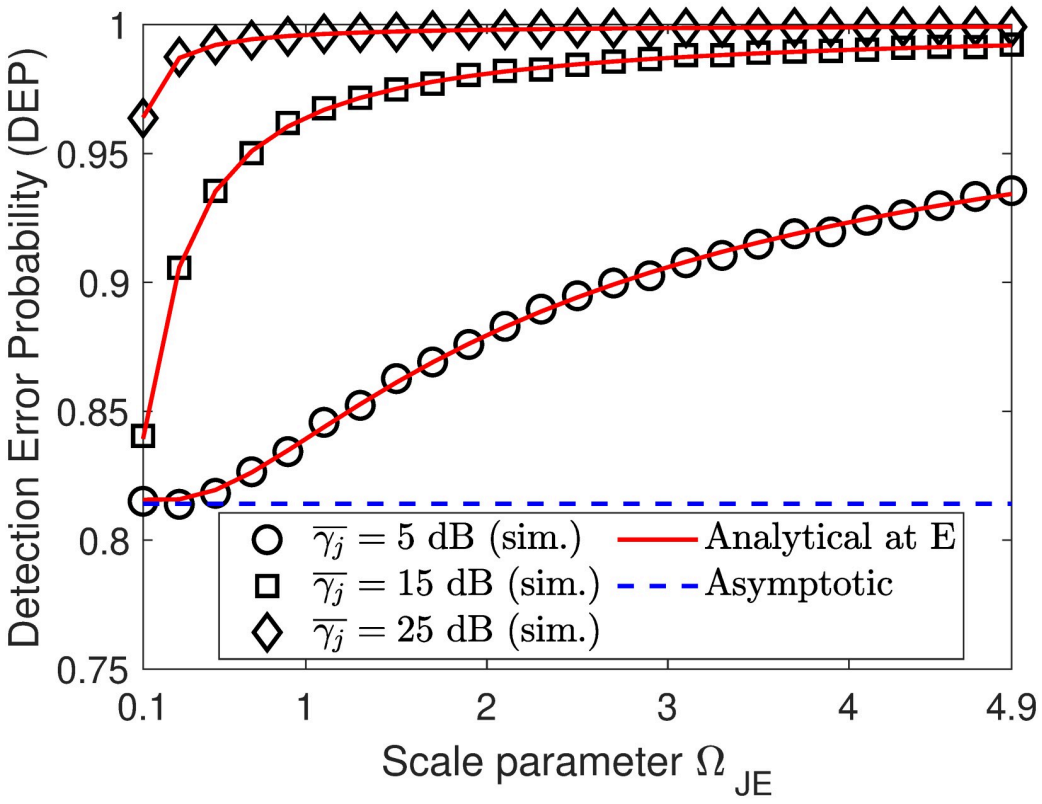


**Fig 6. Impact of fading parameter $\Omega_{\mathsf{JE}}$ on DEP performance.** Setups: $\rho = 0.6$, $\bar{\gamma}_s = 10$ dB, and $\zeta = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g006

where constraints in (37b) refers to the minimal OP of $\mathsf{U}_2$, the minimal SOP of $\mathsf{E}$, and the minimal DEP of $\mathsf{E}$, while constraints in (37c) is the operating condition.

**3.2.2 Solution approach.** Since the problem in (37) involves the complicated expression $\mathrm{DEP}_{\mathsf{E}}^{\star}$, finding the exact optimal PA solution $\rho^{\star}$ is an extremely intricate task. We therefore overcome this challenge by leveraging the connection $\widetilde{\mathrm{DEP}}_{\mathsf{E}}^{\star} \leq \mathrm{DEP}_{\mathsf{E}}^{\star}$. This enables us to simplify the optimization problem in (37) into a tractable problem by checking the feasible domain of $\rho$.

Specifically, we begin with revisiting **Remarks** 1, 3, and 7, where we can obtain: $\widetilde{\mathrm{DEP}}_{\mathsf{E}}^{\star}$ and $\mathrm{SOP}_{\mathsf{E}}$ are an increasing function of $\rho$, respectively, while $\mathrm{OP}_{\mathsf{U}_2}$ is a decreasing function of $\rho$. Based on this, we solve $\mathrm{SOP}_{\mathsf{E}} \leq \epsilon_{\mathsf{E}}$ to get the second feasible region as

$$\rho \leq \underbrace{1 + \frac{\phi}{\bar{\gamma}_s \Omega_{\mathsf{SU}_1} \ln\left(\frac{1-\epsilon_{\mathsf{E}}}{\Xi}\right)}}_{\triangleq \theta}, \tag{38}$$

and solve $\widetilde{\mathrm{DEP}}_{\mathsf{E}}^{\star} \geq \varrho_{\mathsf{U}_2}$ to get the following inequality

$$f(\rho) \triangleq \rho^{1/(1-\rho)} - \rho^{\rho/(1-\rho)} + 1 - \varrho_{\mathsf{U}_2} \geq 0. \tag{39}$$

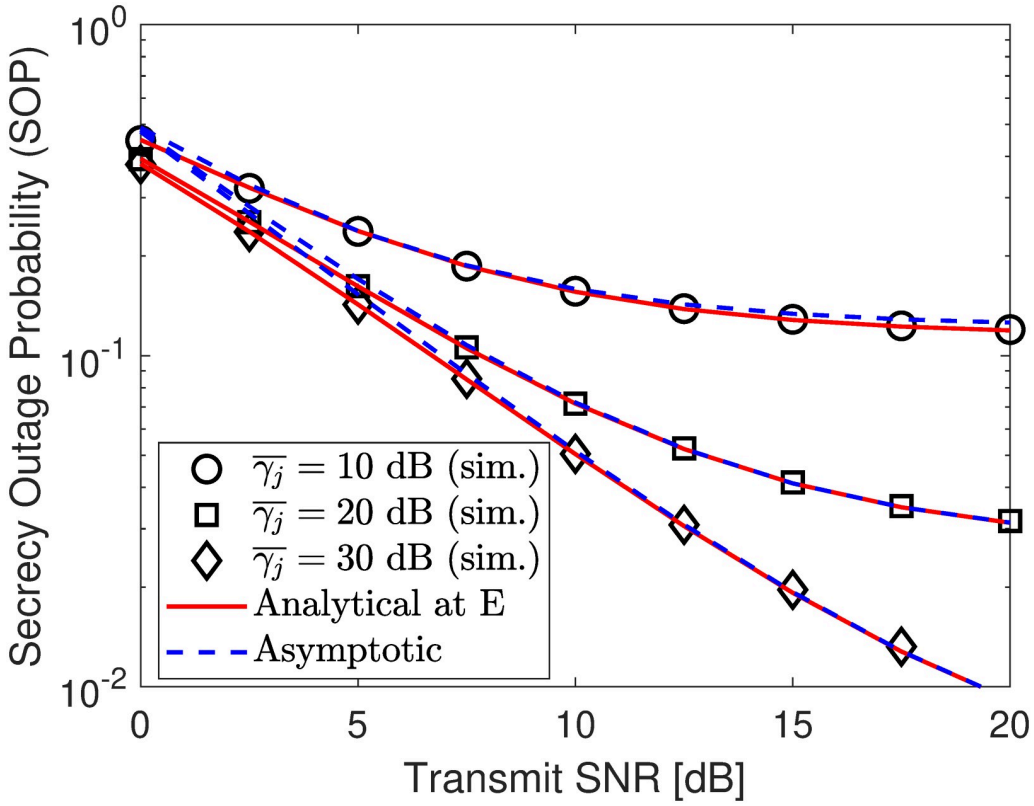


**Fig 7. Impact of $\rho$ (PA coefficient of $\mathsf{U}_2$) on SOP performance under eavesdropping scenario.** Setups: a) $R_1 = r_2 = 0.25$ bps/Hz and $\rho = 0.6$, b) $r_2 = 0.25$ bps/Hz, $\bar{\gamma}_j = 10$ dB, and $\rho = 0.6$, and c) $R_1 = r_2 = 0.25$ bps/Hz and $\bar{\gamma}_j = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g007

However, finding the exact solution for (39) is extremely difficult; thus, we rely on Newton's method for finding a root $\rho^+$ of a function $f(\rho) = 0$, which has derivative

$$f'(\rho) = \ln(\rho)\rho^{\frac{\rho}{1-\rho}}/(\rho - 1). \tag{40}$$

Thus, the fourth feasible region for (39) can be deduced as

$$\rho \geq \rho^+. \tag{41}$$

Next, we solve $\mathrm{OP}_{\mathsf{U}_2} \leq \varepsilon_{\mathsf{U}_2}$ to have the following inequality

$$\rho \geq \underbrace{\frac{\kappa_2}{(1+\kappa_2)} - \frac{\kappa_2}{(1+\kappa_2)\Omega_{\mathsf{SU}_2}\bar{\gamma}_s \ln(1-\varepsilon_{\mathsf{U}_2})}}_{\triangleq \varkappa}. \tag{42}$$

To proceed, we move on exploring the objective function $\mathrm{OP}_{\mathsf{U}_1}$ in (37a) and we notice that it is only improved if (24) holds. Combining this with (37c), we get the feasible region

$$\varphi \leq \rho \leq \xi, \tag{43}$$

where $\varphi \triangleq \max\{\kappa_2/(1+\kappa_2) + \ell, 0.5 + \ell\}$ and $\xi \triangleq \min\{\kappa_2(1+\kappa_1)/(\kappa_1(1+\kappa_2)+\kappa_2), 1-\ell\}$.

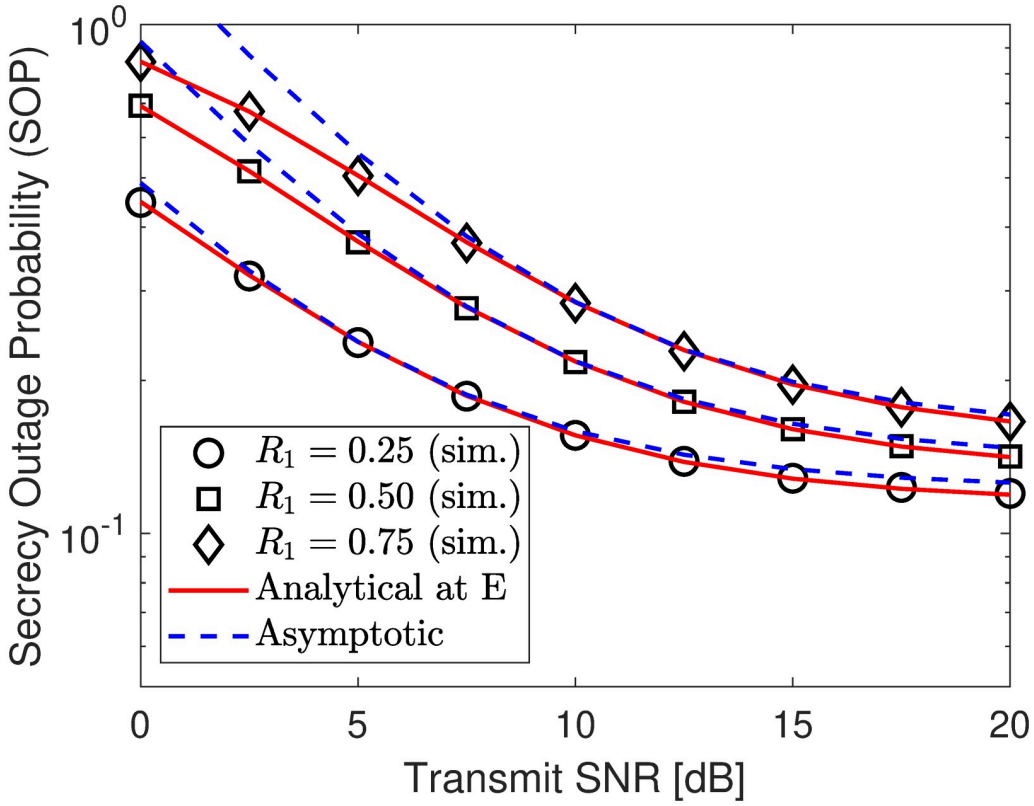


**Fig 8. Impact of $R_1$ (secure rate of $U_1$) on SOP performance under eavesdropping scenario.** Setups: a) $R_1 = r_2 = 0.25$ bps/Hz and $\rho = 0.6$, b) $r_2 = 0.25$ bps/Hz, $\bar{\gamma}_j = 10$ dB, and $\rho = 0.6$, and c) $R_1 = r_2 = 0.25$ bps/Hz and $\bar{\gamma}_j = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g008

Putting (38) and (41)–(43) together, we obtain the sub-optimal solution for (37) as

$$\rho^{\star} = \begin{cases} \min\{\theta, \xi\}, & \max\{\varphi, \rho^{+}, \varkappa\} \leq \min\{\theta, \xi\}, \\ \text{No solution}, & \max\{\varphi, \rho^{+}, \varkappa\} > \min\{\theta, \xi\}. \end{cases} \tag{44}$$

### 3.3 Covert rate maximization

Having all the expressions of the lower-bound optimal DEP, the SOP, and the ergodic rate metrics in hand, in this section, we will first formulate the problem of optimizing resource power allocation subject to maximize the covert rate of sending covert information while ensuring reliable communication of public signal at all legitimate users as well as two lines of security countermeasures for the physical layer transmission. Afterward, we will provide detailed guidance in achieving closed-form sub-optimal PA policy.

**3.3.1 Problem formulation.** This section aims to optimize $\rho$ to maximize the covert rate of $U_1$ while ensuring the systems' security and covert requirements. Specifically, the

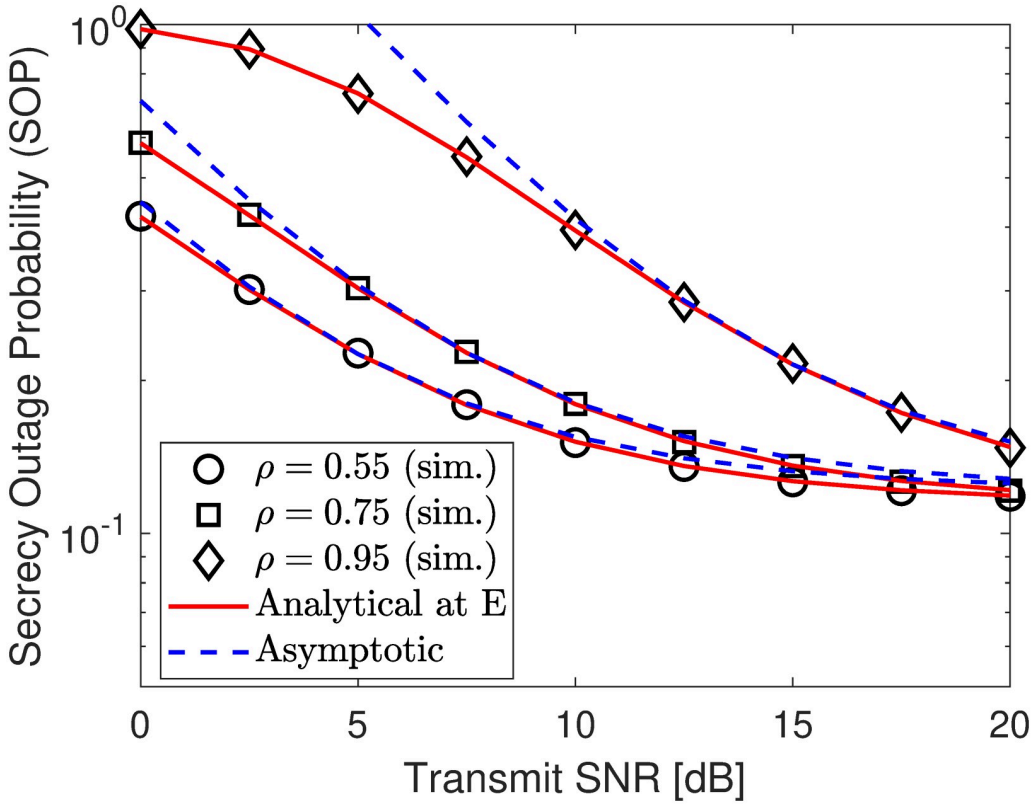


**Fig 9. Impact of $\rho$ (PA coefficient of $\mathsf{U}_2$) on SOP performance under eavesdropping scenario.** Setups: a) $R_1 = r_2 = 0.25$ bps/Hz and $\rho = 0.6$, b) $r_2 = 0.25$ bps/Hz, $\bar{\gamma}_j = 10$ dB, and $\rho = 0.6$, and c) $R_1 = r_2 = 0.25$ bps/Hz and $\bar{\gamma}_j = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g009

optimization problem can be formulated as

$$\max_{\rho} \mathcal{R}_{\mathsf{U}_1} \tag{45a}$$

$$\text{s.t} \;\; \text{SOP}_{\mathsf{E}} \leq \epsilon_{\mathsf{E}}, \text{DEP}^{\star}_{\mathsf{E}} \geq \varrho_{\mathsf{U}_2}, \tag{45b}$$

$$\text{OP}_{\mathsf{U}_1} \leq \boldsymbol{\varepsilon}_{\mathsf{U}_1}, \text{OP}_{\mathsf{U}_2} \leq \boldsymbol{\varepsilon}_{\mathsf{U}_2}, \tag{45c}$$

$$\rho \geq \kappa_2/(1+\kappa_2) + \ell, 1 - \ell \geq \rho \geq 0.5 + \ell, \ell \simeq 0, \tag{45d}$$

where $\boldsymbol{\varepsilon}_{\mathsf{U}_1}$ is the minimum OP required for $\mathsf{U}_1$.

**3.3.2 Solution approach.** Since the complex results of (45a) and $\text{DEP}^{\star}_{\mathsf{E}} \geq \varrho_{\mathsf{U}_2}$ in (45d) makes obtaining the optimal solution for the problem in (45), we tackle this problem by leveraging the connection $\widetilde{\text{DEP}^{\star}_{\mathsf{E}}} \leq \text{DEP}^{\star}_{\mathsf{E}}$, providing the feasible region in (42). Next, we solve $\text{SOP}_{\mathsf{E}} \leq \epsilon_{\mathsf{E}}$ and $\text{OP}_{\mathsf{U}_2} \leq \boldsymbol{\varepsilon}_{\mathsf{U}_2}$, returning the respective results in (38) and (43). Meanwhile,

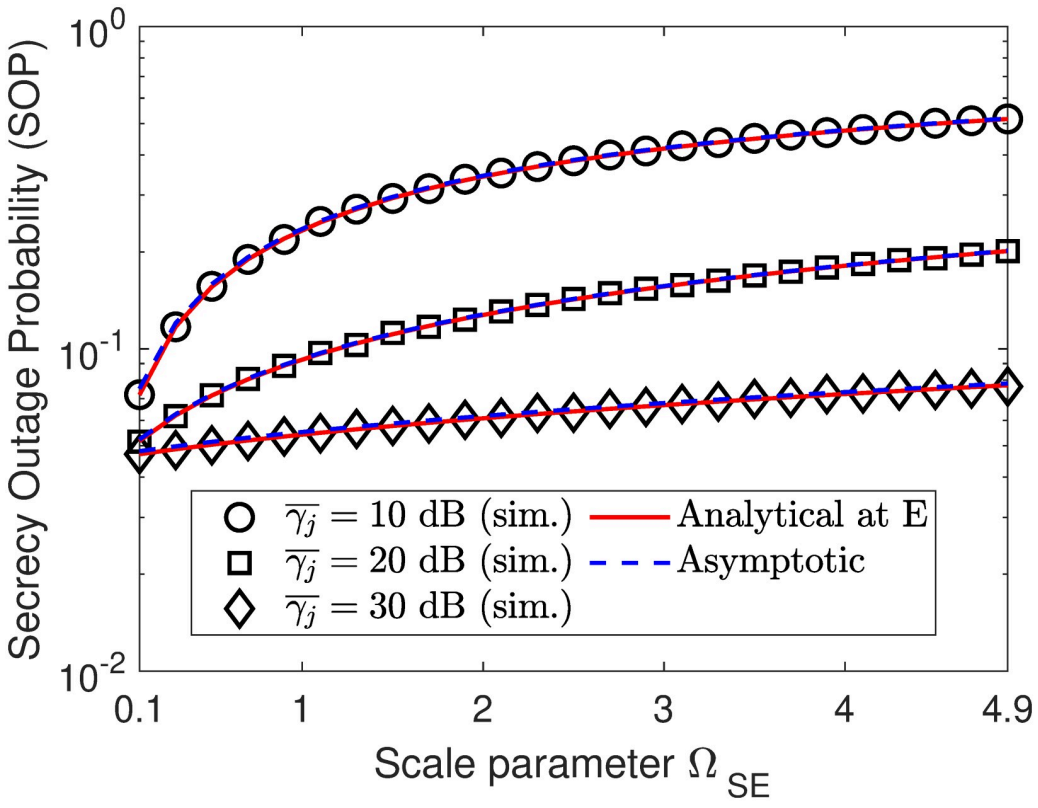


**Fig 10. Impact of fading parameter $\Omega_{SE}$ on SOP performance.** Setups: $R_1 = r_2 = 0.25$ bps/Hz, $\rho = 0.6$, and $\bar{\gamma}_s = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g010

solving $\mathrm{OP}_{\mathrm{U}_1} \leq \varepsilon_{\mathrm{U}_1}$ results in

$$\begin{aligned} & 1-\exp\left(-\frac{1}{\bar{\gamma}_s\Omega_{\mathrm{SU}_1}}\max\{\frac{\kappa_2}{\psi},\frac{\kappa_1}{1-\rho}\}\right) \leq \varepsilon_{\mathrm{U}_1} \\ \Rightarrow & \begin{cases} \rho \geq \dfrac{\kappa_2}{(1+\kappa_2)} - \dfrac{\kappa_2}{\bar{\gamma}_s\Omega_{\mathrm{SU}_1}(1+\kappa_2)\ln(1-\varepsilon_{\mathrm{U}_1})}, & \rho \leq \varpi, \\ \rho \leq 1 + \dfrac{\kappa_1}{\bar{\gamma}_s\Omega_{\mathrm{SU}_1}\ln(1-\varepsilon_{\mathrm{U}_1})}, & \rho > \varpi. \end{cases} \\ \Rightarrow & \underbrace{1+\frac{\kappa_1/[\bar{\gamma}_s\Omega_{\mathrm{SU}_1}]}{\ln(1-\varepsilon_{\mathrm{U}_1})}}_{\triangleq \vartheta_h} \geq \rho \geq \underbrace{\frac{\kappa_2}{(1+\kappa_2)}\left[1-\frac{1/[\bar{\gamma}_s\Omega_{\mathrm{SU}_1}]}{\ln(1-\varepsilon_{\mathrm{U}_1})}\right]}_{\triangleq \vartheta_l}. \end{aligned} \tag{46}$$

Besides, from (45d), (38), (42), (43), and (46), we can deduce the feasible region for $\rho$ as

$$\underbrace{\max\{\varphi,\rho^+,\varkappa,\vartheta_l\}}_{\triangleq \rho_l} \leq \rho \leq \underbrace{\min\{1-\ell,\theta,\vartheta_h\}}_{\triangleq \rho_h}. \tag{47}$$

On the other hand, we get that $\mathcal{R}_{\mathrm{U}_1}$ is a decreasing function of $\rho$ as stated in **Remark** 6. Thus, $\rho$ should be designed with a small value within the feasible region. By combining (46)

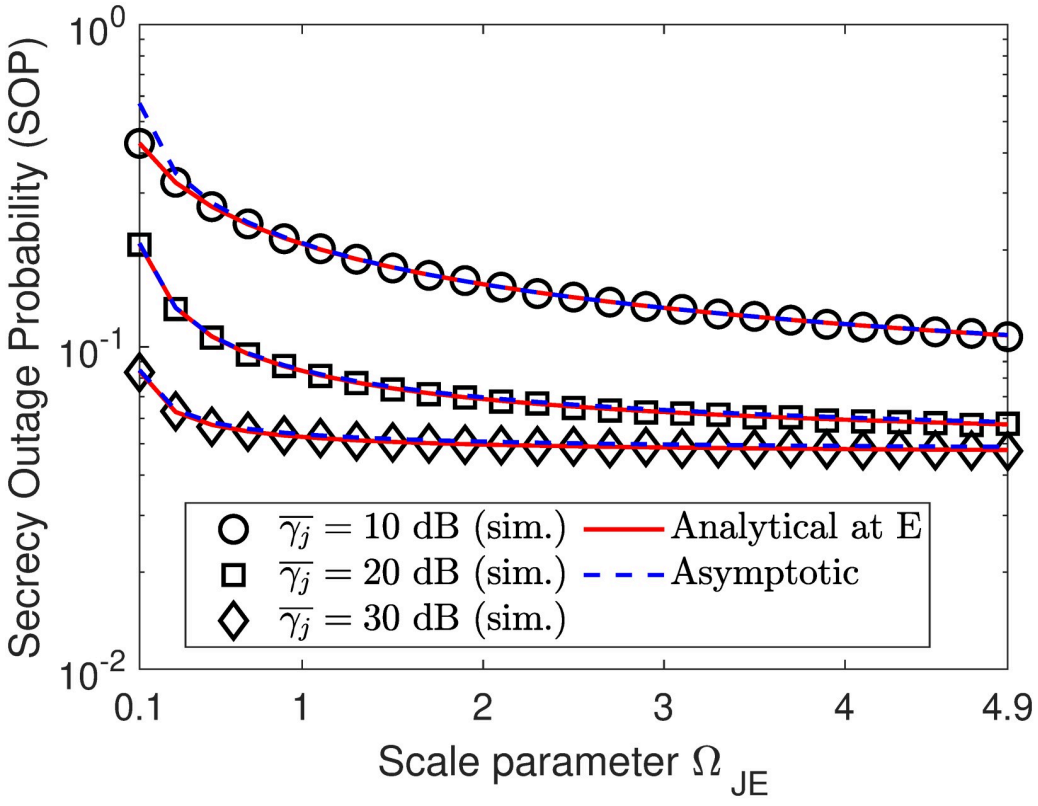


**Fig 11. Impact of fading parameter $\Omega_{JE}$ on SOP performance.** Setups: $R_1 = r_2 = 0.25$ bps/Hz, $\rho = 0.6$, and $\bar{\gamma}_s = 10$ dB.

https://doi.org/10.1371/journal.pone.0317289.g011

and (47), the sub-optimal solution for the problem in (45) can be deduced as

$$\rho^{\star} = \begin{cases} \rho_l, & \rho_l \leq \rho_h, \\ \text{No solution}, & \rho_l > \rho_h. \end{cases} \tag{48}$$

## 4 Numerical results and discussions

In this section, we provide some numerical examples using the Monte-Carlo simulation with $10^4$ trials to validate the designed frameworks in the previous section. Specifically, we set the parameters throughout this section: $\sigma^2 = 1$, $\Omega_{SU_2} = \Omega_{JE} = 0.5$, and $\Omega_{SU_1} = \Omega_{SE} = 1$.

### 4.1 Monitoring scenario

In Figs 2–4, the DEP of monitoring covert transmission between S and $U_1$ for different adjustment activity of E to achieve the minimal DEP. As observed, both the simulation and analytical results in (10) are precisely consistent. Besides, we can find that the DEP has a downtrend with an increase in $\zeta$ and then becomes an uptrend in contrast. The reason is that when $\zeta$ increases, the probability of no transmission observed by E decreases but the probability of existent transmission of $x_1$ observed by E increases and then the former becomes smaller than the latter, yielding an increase in DEP overall. Especially when they intersect, DEP reaches its minimum value, forming a downward concave shape. Fig 2 paints the DEP when $\bar{\gamma}_j =$

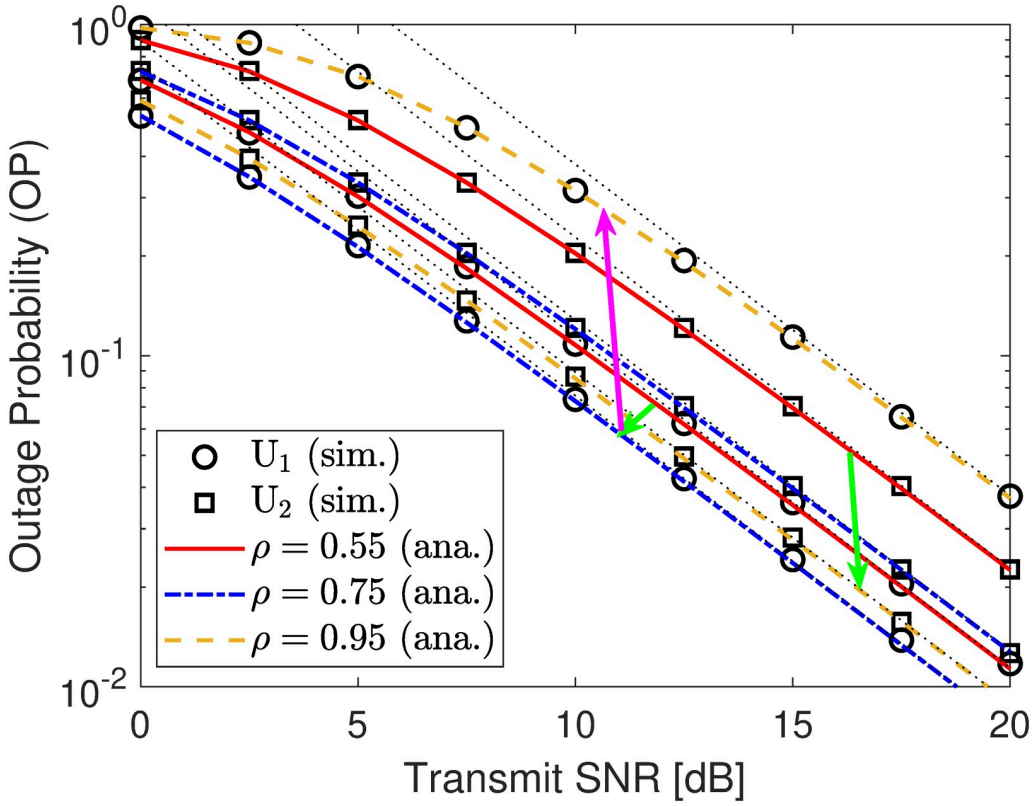


**Fig 12. OP versus SNR $\bar{\gamma}_s$.** Setups: a) $r_1 = 0.25$ and $r_2 = 0.5$.

https://doi.org/10.1371/journal.pone.0317289.g012

5, 10, 15 dB. The results show that the amount of noise SNR strongly affects the DEP performance. When $\bar{\gamma}_j$ increases, E faces more error-prone in covert signal detection, yielding better covert protection of communication for the main system. Especially, we can see that the developed lower bound in (11) is almost lower than the minimal DEP, showing our correct mathematical development. Fig 3 shows the DEP with different values of power distribution coefficients $\rho$. It is observed that the higher the value of $\rho$, the larger the higher DEP performance. It can be concluded that the DEP increases with the increase of $\rho$. The covert performance is improved due to the application of efficient power distribution among NOMA signals that take advantage of user-superimposed messages to make friendly interference. Moreover, from Fig 4, we can further observe that when the transmit SNR $\bar{\gamma}_s$ increases, E must increase its threshold judgment to adapt to this change and from the developed asymptotic result, we can readily discover the minimum DEP that E can achieve without challenging.

In Figs 5 and 6, we plot the DEP performance as a function of either $\Omega_{SE}$ or $\Omega_{JE}$. From Fig 5, we can observe that when $\Omega_{SE}$ increases, the DEP curves has downtrend with variations of $\Omega_{SE}$ from 0.1 to 1 and uptrend with variations of $\Omega_{SE}$ beyond 1. Meanwhile, the result in Fig 6 reveals that the DEP curves almost increase with an increase in fading parameter $\Omega_{JE}$. This is because the larger the value of $\Omega_{JE}$, the stronger the channel interference from the jammer node to the eavesdropper. Besides, we can also observe that increasing the jamming SNR $\bar{\gamma}_j$ plays an important role in increasing the DEP at the eavesdropper.

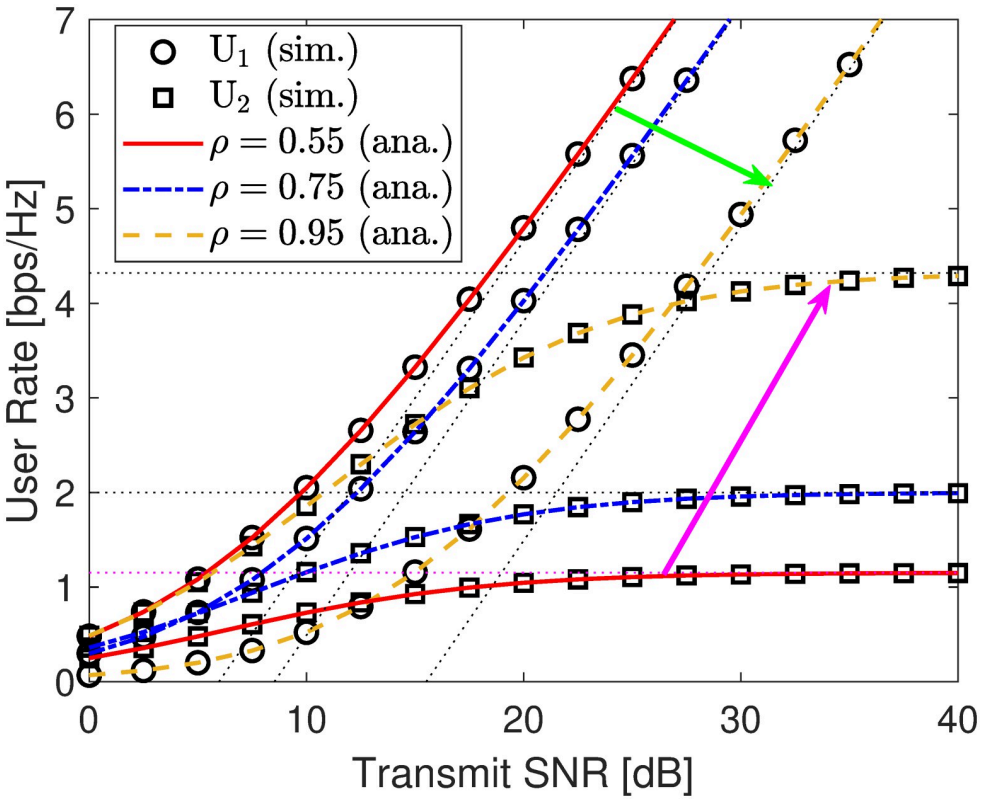


**Fig 13. User rate versus SNR $\bar{\gamma}_s$.** Setups: a) $r_1 = 0.25$ and $r_2 = 0.5$.

https://doi.org/10.1371/journal.pone.0317289.g013

### 4.2 Eavesdropping scenario

Next, we depict the SOP under different jamming power levels in Fig 7, different target security rates in Fig 8, and other PA coefficient in Fig 9. According to the numerical results, no matter what SNR varies, the developed analytical results in (17) perfectly match with the simulation ones and approach the asymptotic plotted using (20) at high SNR region, verifying our developed analytical frameworks. According to the results in Fig 7, it can be seen that the security performance begins to improve and saturates the security floor with $\bar{\gamma}_j = 10$ dB when $\bar{\gamma}_s$ exceeds 10 dBm. However, we can surpass this challenge by increasing jamming signal levels, i.e., $\bar{\gamma}_j$, to produce more interference to confuse E's information extraction, strengthening the SOP significantly. Therefore, deploying a jammer has a splendid impact on security performance.

In Figs 10 and 11, we plot the SOP performance as a function of either $\Omega_{SE}$ or $\Omega_{JE}$. Specifically, we can observe that there is an opposite SOP trend between Figs 10 and 11, where the SOP in Fig 10 tends to increase with the increment of $\Omega_{SE}$, while that of Fig 11 tends to decrease with the increment of $\Omega_{JE}$. This is because when the eavesdropper is close to the source information (i.e., $\Omega_{SE}$ is increased), its channel gain becomes better and thus covert information of Bob can be decoded with higher probability. Meanwhile, increasing $\Omega_{JE}$ results in higher channel interference on the reception of the eavesdropper, thus degrading its decoding ability and improving the SOP accordingly. However, both also have the same trend is that increasing the jamming SNR $\bar{\gamma}_j$ helps improve the SOP performance, which is true with the expected role of the jamming node.

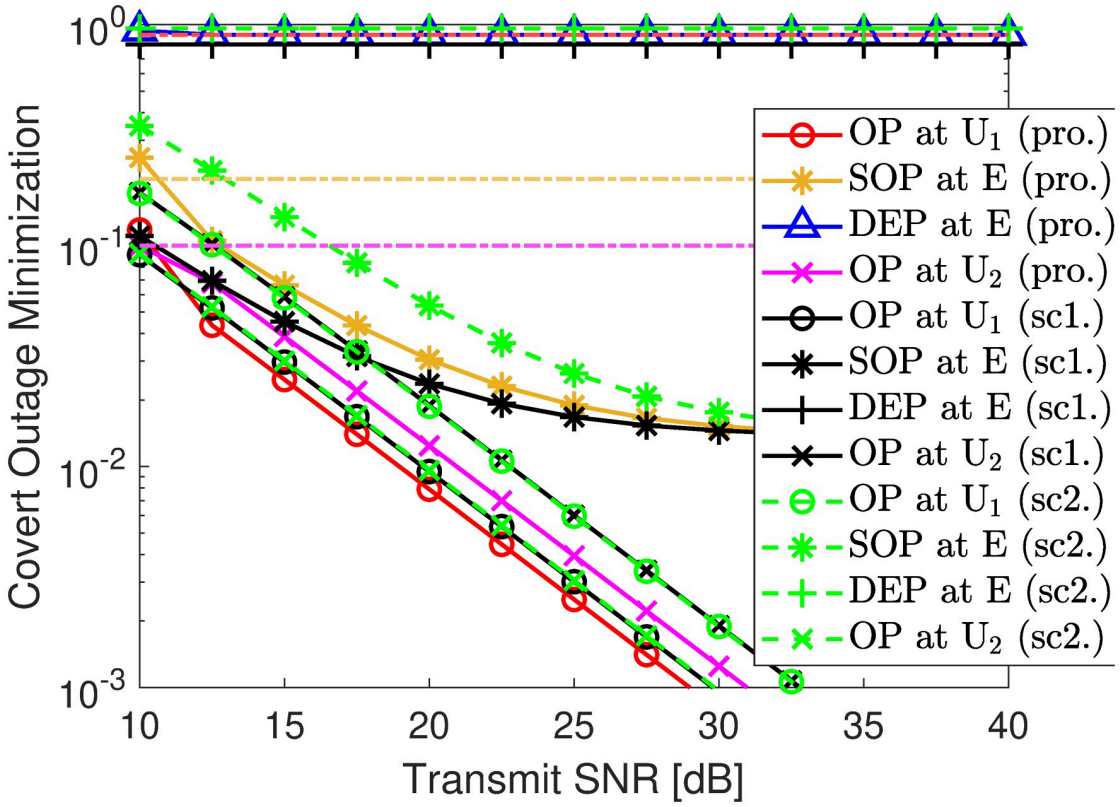


**Fig 14. Cover outage optimization versus SNR $\bar{\gamma}_s$.** Setups: a) $r_1 = 0.25$ bps/Hz, $R_1 = r_2 = 0.5$ bps/Hz, $\bar{\gamma}_j = 30$ dB, and $\ell = 10^{-3}$. b) $r_1 = 0.5$ bps/Hz, $R_1 = 0.25$ bps/Hz, $\bar{\gamma}_j = 30$ dB, and $\ell = 10^{-3}$.

https://doi.org/10.1371/journal.pone.0317289.g014

### 4.3 User performance

**4.3.1 Outage and rate analysis.** We investigate the relationship between the transmit SNR $\bar{\gamma}_s$ and the users' OPs and rates. From Fig 12, it can be seen that no matter what the SNR changes, the OP curves improve considerably, and both simulation and analytical results are consistent with each other, showing the correctness of our derived expressions in (23) and (31). Besides, at high SNR, the asymptotic results (dot lines) can accurately predict the simulation ones, showing the correctness of (25) and (32). Moreover, we can further find from Fig 12 that the OP of $\mathsf{U}_2$ almost improves with $\rho = 0.55, 0.75, 0.95$ when $\bar{\gamma}_s$ is constant. Conversely, the OP of $\mathsf{U}_1$ has a downtrend with $\rho = 0.55, 0.75$ but an uptrend with $\rho = 0.95$. These observations are almost aligned with analyses in **Remarks** 4 and 7. Therefore, optimizing the power distribution coefficient $\rho$ is a critical task. Next, from Fig 13, we can obtain the covert rate of $\mathsf{U}_1$ corresponding to the linear curve of $\bar{\gamma}_s$ to its asymptote, where increasing $\bar{\gamma}_s$ has a strong effect in boosting the covert transmission rate. However, the rate of $\mathsf{U}_2$ corresponds to the curve of $\bar{\gamma}_s$ to its asymptote, at which point increasing $\bar{\gamma}_s$ has almost no effect on the public transmission rate. However, when we increase the power distribution coefficient $\rho$, the public transmission rate improves considerably. Unfortunately, such configurations decline the quality of the covert transmission rate, yielding a trade-off in covert and public transmission rates between users.

**4.3.2 Covert outage minimization and rate maximization.** In Fig 14, the OP of transmitting a covert signal at $\mathsf{U}_1$ is described as a function of the transmit $\bar{\gamma}_s$. By comparing two

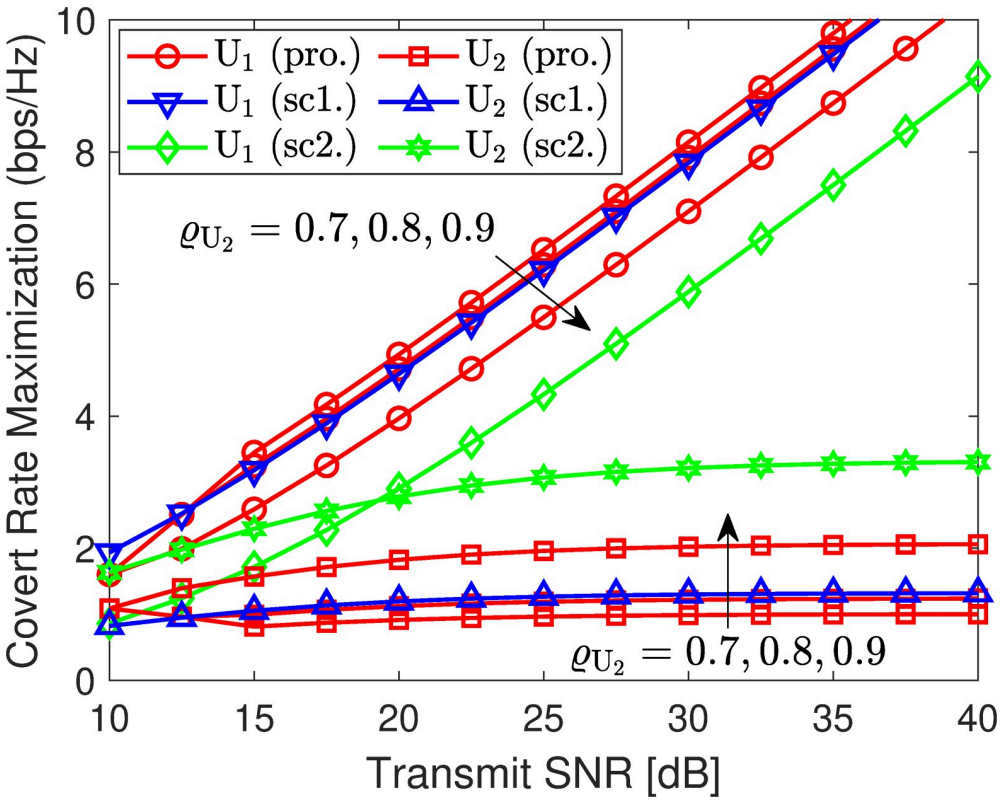


**Fig 15. User rate optimization versus SNR $\bar{\gamma}_s$.** Setups: a) $r_1 = 0.25$ bps/Hz, $R_1 = r_2 = 0.5$ bps/Hz, $\bar{\gamma}_j = 30$ dB, and $\ell = 10^{-3}$. b) $r_1 = 0.5$ bps/Hz, $R_1 = 0.25$ bps/Hz, $\bar{\gamma}_j = 30$ dB, and $\ell = 10^{-3}$.

https://doi.org/10.1371/journal.pone.0317289.g015

schemes of fixed PA scheme 1 (sc1.): $\rho = 0.6$ and scheme 2 (sc2.): $\rho = 0.9$. Under the constants for designing security $\epsilon_{\mathsf{E}} = 0.2$ (yellow dash-dot line), covert $\varrho_{\mathsf{U}_2} = 0.9$ (red dash-dot line), and reliability transmission $\varepsilon_{\mathsf{U}_2} = 0.1$ (pink dash-dot line), it can be seen that scheme 1 can satisfy the SOP at $\mathsf{E}$ and OP at $\mathsf{U}_2$ with $\bar{\gamma}_s > 12.5$ dB but violate the DEP requirement at $\mathsf{E}$. Meanwhile, scheme 2 satisfies the SOP at $\mathsf{E}$ but requires $\bar{\gamma}_s > 17.5$ dB to meet the OP at $\mathsf{U}_2$ and $\bar{\gamma}_s > 10$ dB to meet the SOP at $\mathsf{E}$. Especially, compared to scheme 1, scheme 2 offers a better OP performance for $\mathsf{U}_2$ but a lower OP performance for $\mathsf{U}_1$. This trend is similar to that of Fig 14. This confirms the fact that distributing the coefficient $\rho$ plays an important role in ensuring the system's overall performance. With the proposed solution in (44), our approach does not only satisfy the DEP, SOP, and OP requirements but also improves the OP of $\mathsf{U}_1$ considerably while achieving the OP of $\mathsf{U}_2$ very close to that of scheme 2.

In Fig 15, the covert rate of $\mathsf{U}_1$ is plotted as a function of the transmit $\bar{\gamma}_s$. As observed, exploiting scheme 2 provides a public rate for $\mathsf{U}_2$ higher than Scheme 1 but results in a lower covert rage for $\mathsf{U}_1$, and vice versa. However, schemes 1 and 2 do not consider the OP, SOP, and DEP requirements. Thus, if these constraints are accounted for covert communication and our proposed method in (48) is used, we can observe that when the target covert rate of $\varrho_{\mathsf{U}_2}$ is small, the system has great change to allocate higher power level to enhance $\mathsf{U}_1$'s covert rate. Specifically, when $\varrho_{\mathsf{U}_2} = 0.7$, the covert rate of $\mathsf{U}_1$ can enhance up to 0.5 bps/Hz compared to Scheme 1 and 2 bps/Hz over Scheme 2. However, $\varrho_{\mathsf{U}_2} = 0.9$, the covert rate of $\mathsf{U}_1$ is decreased since a lower PA level is required to meet the DEP demand as analyzed in **Remark**

1. Although the covert rate of $U_2$ is decreased, it remains higher than Scheme 2 and the public rate is indeed better than that of Scheme 1. These show that our proposed approach can efficiently capture the security risks and provide sustainable transmission with specific network conditions.

## 5 Conclusion

This work provided a comprehensive analysis of the NOMA system with users and external eavesdroppers in terms of outage transmission, secrecy outage performance and detection error. Under artificial noise generated by the jammer, closed-form for the OP, SOP, and DEP had been derived in terms of exact and asymptotic manner. Moreover, the covert and public rate formulas were also derived in exact and asymptotic. To enhance covert transmission, two optimization problems of covert outage minimization and covert rate maximization subject to the OP, SOP, and DEP requirements had been formulated and addressed, where we relied on the developed OP, SOP, and DEP to find the sub-optimal PA coefficient by closed-form expressions. Finally, we validated the developed mathematical and optimization frameworks by numerical results. Some key findings can be deduced from investigations of numerical result studies as follows:

1. Deploying the jamming node plays an important role in preventing potential external eavesdroppers. Specifically, increasing the jamming power not only causes more errors for the monitoring but also eavesdropping, leading to higher DEP and smaller SOP performances, respectively.
2. There exists a trade-off in allocating the transmit power between public and covert signals, where increasing the PA coefficient $\rho$ almost improves the OP of $U_2$ but it yields a down-up trend on the OP of $U_1$. As for the ergodic rate aspect, increasing the PA coefficient $\rho$ helps increase the capacity of $U_2$ but decreases that of $U_1$.
3. Given a fixed jamming power constraint, by exploring our proposed approach, the system can significantly improve the OP/cover rate of covert communication while ensuring the performance requirements of the OP of users, the SOP, and the DEP.

Since there is still much room that has not been covered yet, it is interesting to further investigate in the near future works, such as multi-antenna transmission, generalized channel models (e.g., Nakgami-m or Rician), untrusted near–trusted far user scenarios, multi eavesdroppers with colluding and non-colluding situations, imperfect channel estimation, and the issues of joint secure and covert energy efficiency. Besides, extending this study to backscatter communication [30] along with coverage enhancement with a reconfigurable surface can be regarded as a great potential direction for less-battery networks.

## Supporting information

**S1 File. The simulation code used in this work can be found at: MatlabCode.**
(ZIP)

## Author Contributions

**Data curation:** Thanh Binh Doan.

**Formal analysis:** Thanh Binh Doan.

**Methodology:** Tien-Hoa Nguyen.

**Resources:** Thanh Binh Doan.

**Supervision:** Tien-Hoa Nguyen.

**Visualization:** Thanh Binh Doan.

**Writing – original draft:** Thanh Binh Doan.

**Writing – review & editing:** Tien-Hoa Nguyen.

## References

1. Aouedi O, Vu TH, Sacco A, Nguyen DC, et al. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. IEEE Commun Surv Tutorials. 2024. https://doi.org/10.1109/COMST.2024.3430368
2. Chen X, An J, Xiong Z, Xing C, Zhao N, Yu FR, et al. Covert Communications: A Comprehensive Survey. IEEE Commun Surv Tut. 2023; 25(2):1173–1198. https://doi.org/10.1109/COMST.2023.3263921
3. Xing L. Reliability in Internet of Things: Current Status and Future Perspectives. IEEE IoT J. 2020; 7 (8):6704–6721.
4. Hu J, Lin C, Li X. Relationship Privacy Leakage in Network Traffics. In: 2016 25th Int. Conf. Comput. Commun. Netw. (ICCCN). Waikoloa, HI, USA; 2016. p. 1–9.
5. Yuan Y, Wang S, Wu Y, Poor HV, Ding Z, You X, et al. NOMA for Next-Generation Massive IoT: Performance Potential and Technology Directions. IEEE Commun Mag. 2021; 59(7):115–121. https://doi.org/10.1109/MCOM.001.2000997
6. Shahab MB, Abbas R, Shirvanimoghaddam M, Johnson SJ. Grant-Free Non-Orthogonal Multiple Access for IoT: A Survey. IEEE Commun Surv Tut. 2020; 22(3):1805–1838. https://doi.org/10.1109/COMST.2020.2996032
7. Chen X, Jia R, Ng DWK. On the Design of Massive Non-Orthogonal Multiple Access With Imperfect Successive Interference Cancellation. IEEE Trans Commun. 2019; 67(3):2539–2551. https://doi.org/10.1109/TCOMM.2018.2884476
8. Vu TH, Pham QV, Nguyen TT, da Costa DB, Kim S. Enhancing RIS-Aided Two-Way Full-Duplex Communication With Non-Orthogonal Multiple Access. IEEE IoT J. 2024; 11(11):19963–19977.
9. Nguyen TT, Vu TH, Tu LT, Duy TT, Nguyen QS, da Costa DB. A Low-Complexity Relaying Protocol for Cooperative Short-Packet NOMA-based Spectrum Sharing Systems. IEEE Trans Veh Technol. Jun 2024; 73. https://doi.org/10.1109/TVT.2023.3348633
10. Aghdam MRG, Tazehkand BM, Abdolee R. On the Performance Analysis of mmWave MIMO-NOMA Transmission Scheme. IEEE Trans Veh Technol. 2020; 69(10):11491–11500. https://doi.org/10.1109/TVT.2020.3012516
11. Aghdam MRG, Tazehkand BM, Abdolee R, Feghhi MM. Space-Time Block Coding in Millimeter Wave Large-Scale MIMO-NOMA Transmission Scheme. Int J Commun Syst. 2020; 33(9):e4392. https://doi.org/10.1002/dac.4392
12. Aghdam MRG, Tazehkand BM, Abdolee R. Joint Optimal Power Allocation and Beamforming for MIMO-NOMA in mmWave Communications. IEEE Wireless Commun Lett. 2022; 11(5):938–941. https://doi.org/10.1109/LWC.2022.3150217
13. Le AT, Tran DH, Le CB, Tin PT, Nguyen TN, et al. Power Beacon and NOMA-Assisted Cooperative IoT Networks With Co-Channel Interference: Performance Analysis and Deep Learning Evaluation. IEEE Trans Mob Comput. 2023; 23(6):7270–7283. https://doi.org/10.1109/TMC.2023.3333764
14. Vu TH, Nguyen TN, Nguyen TT, Kim S. Hybrid Active-Passive STAR-RIS-based NOMA Systems: Energy/Rate-Reliability Trade-offs and Rate Adaptation. IEEE Wireless Commun Lett. 2024; p. 1. https://doi.org/10.1109/LWC.2024.3497978
15. Vu TH, Pham QV, da Costa DB, Debbah M, Kim S. Physical-Layer Security in Short-Packet NOMA Systems with Untrusted Near Users. In: 2023 IEEE Int. Conf. Commun. Workshop (ICC Workshops). Rome, Italy; 2023. p. 1830–1835.
16. Lei H, Zhu C, Park KH, Lei W, Ansari IS, Tsiftsis TA. On Secure NOMA-Based Terrestrial and Aerial IoT Systems. IEEE IoT J. Arp 2022; 9(7):5329–5343.
17. Xiang Z, Yang W, Cai Y, Xiong J, Ding Z, Song Y. Secure Transmission in a NOMA-Assisted IoT Network With Diversified Communication Requirements. IEEE IoT J. Nov 2020; 7(11):11157–11169.
18. Xiang Z, Yang W, Cai Y, Ding Z, Song Y, Zou Y. NOMA-Assisted Secure Short-Packet Communications in IoT. IEEE Wireless Commun. Aug 2020; 27(4):8–15. https://doi.org/10.1109/MWC.01.1900529

19. Jiang Y, Wang L, Zhao H, Chen HH. Covert Communications in D2D Underlaying Cellular Networks With Power Domain NOMA. IEEE Syst J. 2020; 14(3):3717–3728. https://doi.org/10.1109/JSYST.2020.2967089

20. Tao L, Yang W, Yan S, Wu D, Guan X, Chen D. Covert Communication in Downlink NOMA Systems With Random Transmit Power IEEE Wireless Commun Lett. Nov 2020; 9(11):2000–2004. https://doi.org/10.1109/LWC.2020.3011191

21. Zhang Y, He W, Li X, Peng H, Rabie K, Nauryzbayev G, et al. Covert Communication in Downlink NOMA Systems With Channel Uncertainty. IEEE Sensors J. 2022; 22(19):19101–19112. https://doi.org/10.1109/JSEN.2022.3201319

22. Duan Z, Yang X, Gong Y, Wang D, Wang L. Covert Communication in Uplink NOMA Systems Under Channel Distribution Information Uncertainty. IEEE Commun Lett. May 2023; 27(5):1282–1286. https://doi.org/10.1109/LCOMM.2023.3255838

23. Li Q, Xu D, Navaie K, Ding Z. Covert and Secure Communications in NOMA Networks With Internal Eavesdropping. IEEE Wireless Commun Lett. Dec 2023;. https://doi.org/10.1109/LWC.2023.3312689

24. Park T, Lee G, Saad W, Bennis M. Sum Rate and Reliability Analysis for Power-Domain Nonorthogonal Multiple Access (PD-NOMA). IEEE IoT J. Jun 2021; 8(12):10160–10169.

25. Sreya G, Saigadha S, Mankar PD, Das G, Dhillon HS. Adaptive Rate NOMA for Cellular IoT Networks. IEEE Wireless Commun Lett. Mar 2022; 11(3):478–482. https://doi.org/10.1109/LWC.2021.3132932

26. Vu TH, Kim S. Performance Evaluation of Power-Beacon-Assisted Wireless-Powered NOMA IoT-Based Systems. IEEE IoT J. 2021; 8(14):11655–11665.

27. Vu TH, Nguyen TV, Kim S. Wireless Powered Cognitive NOMA-Based IoT Relay Networks: Performance Analysis and Deep Learning Evaluation. IEEE IoT J. 2022; 9(5):3913–3929.

28. Le AT, Vu TH, Tu NH, Nguyen TN, Tu LT, et al. Active Reconfigurable Repeater-Assisted NOMA Networks in Internet-of-Things: Reliability, Security, and Covertness. IEEE IoT J. 2024; p. 1. https://doi.org/10.1109/JIOT.2024.3503278

29. Jeffrey A, Zwillinger D. Table of integrals, series, and products. Elsevier; 2007.

30. Le AT, Nguyen TN, Tu LT, Tran TP, Duy TT, et al. Performance Analysis of RIS-Assisted Ambient Backscatter Communication Systems. IEEE Wireless Commun Lett. 2023; 13(3):791–795. https://doi.org/10.1109/LWC.2023.3344113