

Pinching Antenna-aided NOMA Systems with Internal Eavesdropping

Haolian Chi, Kunrui Cao, Zhou Su, *Senior Member, IEEE*, Lei Zhou,
 Panagiotis D. Diamantoulakis, *Senior Member, IEEE*, Yuanwei Liu, *Fellow, IEEE*,
 and George K. Karagiannidis, *Fellow, IEEE*

Abstract—As a novel member of flexible antennas, the pinching antenna (PA) is realized by integrating small dielectric particles on a waveguide, offering unique regulatory capabilities on constructing line-of-sight (LoS) links and enhancing transceiver channels, reducing path loss and signal blockage. Meanwhile, non-orthogonal multiple access (NOMA) has become a potential technology of next-generation communications due to its remarkable advantages in spectrum efficiency and user access capability. The integration of PA and NOMA enables synergistic leveraging of PA’s channel regulation capability and NOMA’s multi-user multiplexing advantage, forming a complementary technical framework to deliver high-performance communication solutions. However, the use of successive interference cancellation (SIC) introduces significant security risks to power-domain NOMA systems when internal eavesdropping is present. To this end, this paper investigates the physical layer security of a PA-aided NOMA system where a nearby user is considered as an internal eavesdropper. We enhance the security of the NOMA system through optimizing the radiated power of PAs and analyze the secrecy performance by deriving the closed-form expressions for the secrecy outage probability (SOP). Furthermore, we extend the characterization of PA flexibility beyond deployment and scale adjustment to include flexible regulation of PA coupling length. Based on two conventional PA power models, i.e., the equal power model and the proportional power model, we propose a flexible power strategy to achieve secure transmission. The results highlight the potential of the PA-aided NOMA system in mitigating internal eavesdropping risks, and provide an effective strategy for optimizing power allocation and cell range of user activity.

Index Terms—Pinching antenna, non-orthogonal multiple access, physical layer security, internal eavesdropping.

I. INTRODUCTION

The sixth generation (6G) of wireless networks represents a revolutionary development forward in the evolution of wireless communication technology, transcending the limitations of the fifth generation (5G), to meet the expanding and complex demands of emerging applications. 6G delivers ultra-high data

Haolian Chi, Kunrui Cao, and Lei Zhou are with Information Support Force Engineering University, Wuhan 430035, China, and also with the School of Information and Communications, National University of Defense Technology, Wuhan 430035, China (e-mail: chihaolian20@nudt.edu.cn; krcao@nudt.edu.cn; cat_radar@163.com).

Zhou Su is with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: zhousu@ieee.org).

Panagiotis D. Diamantoulakis, and George K. Karagiannidis are with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Thessaloniki 54124, Greece (e-mail: padiamant@gmail.com; geokarag@auth.gr).

Yuanwei Liu is with the Department of Electrical and Electronic Engineering, the University of Hong Kong, Hong Kong, China (e-mail: yuanwei@hku.hk).

rates, ultra-low latency, and ultra-high reliability, integrating multiple functions including communication, computing, and control [1], [2]. The diverse application scenarios of 6G require not only ultra-reliable and high-capacity communication but also the ability to dynamically shape wireless propagation environments, enabling precise and personalized services for diverse users and scenarios [3]. However, early research based on Shannon’s information theorem treated transceivers as fixed and uncontrollable entities [4], focusing solely on adapting to the electromagnetic environment. These approaches fail to meet the requirements of next-generation communications for shaping the propagation environments. The advent of multiple-input multiple-output (MIMO) challenges this paradigm via spatial multiplexing and beamforming [5], [6]. To realize programmable wireless environments, significant research efforts have focused on the development of flexible antenna technologies, such as reconfigurable intelligent surface (RIS), fluid antenna (FA), and movable antenna (MA), which transformed communication systems from “adapting” to “adjusting” the electromagnetic environment [7]–[9]. A key advantage of these flexible antennas lies in their ability to dynamically reconfigure effective channel gains. Specifically, RIS leverages programmatically controlled reflective components to regulate electromagnetic waves, achieving passive beam shaping and interference mitigation to optimize propagation conditions [7]–[10]. FA can employ reconfigurable substances such as liquid metals or ionized solutions with real-time positional adjustments, providing improved flexibility in signal transmission for devices operating in space-limited environments [8]. MA can adaptively modify their physical locations to change radiation direction and coverage range, enabling responsive adjustments to variations in user positions [9].

However, the above flexible antenna technologies face critical limitations [11]. RIS suffers significant path loss stemming from dual attenuation, the locations of FA and MA systems are usually fixed or limited within the wavelength scale, which have difficulties in combating large-scale path loss, especially when the LoS link is unavailable [12]. Additionally, their limited aperture adjustment range, high manufacturing costs, and deployment procedures hinder their scalability in complex 6G scenarios [13]. These challenges have stimulated research into the pinching antenna (PA) [14]. Distinguished by its unique pinchable structure, PA can reconstruct large-scale channel and reduce path loss. This design converts path loss into a programmable parameter by enabling flexible adjustment of PA placement along the waveguide, thus changing the

distance between radiating points and users. Additionally, this capability allows PA to establish adjustable LoS links even in complex or obstructed environments without requiring extra hardware, making them a practical solution for dynamically shaping wireless propagation.

A. Related Works

PA can establish LoS links through flexible position adjustment and flexibly scale up or down the system size. These advantages have stimulated research on establishing LoS links through the use of PA to enhance the communication performance in communication systems [15], [16]. In [15], the basic structure and working principle, as well as the signal model in PA-aided systems were introduced. The authors in [17] have verified the superior performance of PA compared to the traditional fixed antennas by analyzing the performance in different scenarios. In [18], the array gain achieved by PA technology was analyzed. The derived closed-form upper bound for array gain shows that it does not always increase monotonically with the number of PA or with decreasing PA spacing. Instead, the optimal number of antennas and spacing must be determined. In [19], the waveguide attenuation was considered to derive closed-form expressions for outage probability and average rate of PA systems. The above works focused on PA-aided downlink communications. In [20], [21], the uplink communication aided by PAs was investigated. For the first time, the uplink performance optimization of multi-user PA systems was investigated in [20], where it has achieved a balance between throughput and fairness by maximizing the minimum achievable data rate among devices. The authors in [21] evaluated the performance gains of uplink PA communications systems for three scenarios, i.e., multiple PAs for a single user, a single PA for a single user, and a single PA for multiple users. The results have proved that the flexibility of PAs made the communication systems outperform conventional fixed antennas-aided communication systems. Beyond the theoretical performance analysis of PA systems, several optimization problems and corresponding algorithms have been formulated to further enhance the performance of such systems [16], [22]–[24]. The authors in [22] designed scalable codebooks and corresponding three-stage beam training schemes, including non-orthogonal multiple access (NOMA)-aided and dimension-increasing ones for beam training in PA systems under different scenarios, with advantages in reducing training overhead, enhancing flexibility performance, and high-frequency phase alignment. Similarly, issues such as beam training and the joint optimization of antenna position and power have been thoroughly investigated in [23], [24]. In [16], the graph neural network was applied to address the joint optimization of antenna placement and power allocation in PA systems. These studies profoundly verify the flexible regulation characteristics of PA systems, whose performance has achieved a significant improvement compared with conventional antenna systems.

Furthermore, due to the outstanding advantages in spectrum efficiency and user access capability, the NOMA technology has become one of the key technologies for the next-generation

communications. The PA-aided NOMA can fully leverage the channel control capability of the former and the multi-user multiplexing advantage of the latter [12] [15] [17] [22] [25] [26]. The authors in [17] designed a downlink scheme aided by a PA system that supports both orthogonal multiple access and NOMA, derived the upper bound of system performance and verified the significant performance gains of the PA-aided NOMA system. They further pointed out that achieving optimal performance requires sophisticated deployment of antenna positions. To address the antenna deployment issue, [12] proposed a low-complexity placement design for PAs, aiming to maximize the sum rate of multiple downlink users, and discussed the time division multiple access and NOMA schemes in the scenario of single pinching antenna deployment. The problem of antenna activation in NOMA-aided PA systems was studied in [25], aiming to maximize the system throughput. Specifically, the study assumed that the power amplifiers had been installed at preconfigured positions prior to transmission, thereby formulating a joint optimization problem involving the number and deployment locations. Beyond the PA-aided NOMA system with a single waveguide, the scenario with multiple waveguides in the NOMA system was studied in [26]. In this research, a classical power control problem that aims to minimize the total power consumption of all users was formulated. The above research has demonstrated that the two complement each other, forming a high-performance communication solution that provides crucial support for enhancing the 6G communication performance. This integration boasts inherent technical compatibility and substantial research value.

Due to the openness of PA systems, the security of communication systems is exposed to significant risks. The application of physical layer security in PA systems is an effective way to improve the system's security performance. The authors in [13] proposed a gradient method and a fractional programming-based block coordinate descent algorithm for single/multi-user wiretap scenarios to optimize baseband beamforming and PA activation positions. The results demonstrate that flexible PA activation serves as an effective PLS measure, enabling PA systems to outperform conventional fixed antenna systems in terms of security. In [27], the authors studied a classic wiretap scenario where confidential information is transmitted from a base station (BS) to a legitimate user, with an eavesdropper attempting interception. The main destination and eavesdropper have random locations. Results show dynamic PA deployment adjustment enhances security performance, and secrecy capacity improves when PA is placed closer to the destination.

B. Motivation and Contributions

Despite progress in PA-aided NOMA systems and PA-based PLS, critical gaps remain. In particular, the use of successive interference cancellation (SIC) leads to an internal eavesdropping of NOMA with multi-user, where a public information user may overhear the information of confidential information users in the superimposed information streams. However, no relevant research on PA-aided NOMA systems against internal eavesdropping has been reported in the existing literature yet. Existing works, such as [12] [15] [17] [22]

[25] [26], mainly focus on improving the robust performance of PA-aided NOMA systems but overlook the investigation of internal security issues. In the research on PLS for PA systems, the single-waveguide multi-PA systems primarily focus on adjusting the phase of PAs to enhance system security, while the multi-waveguide and multi-PA systems concentrates on optimizing secure beamforming schemes [13], [27]. Current literature universally identifies flexibility as the most significant characteristic of PAs. However, such flexibility is limited to the flexible addition/removal and location deployment of PAs. The two common power models, i.e., the equal power model and the proportional power model fix the radiated power of PAs, which limits the flexibility of their radiated power. These gaps hinder the further development and application of PA-aided NOMA systems in practical secure scenarios. Motivated by the above, we analyze the security performance of PA-aided NOMA systems with internal eavesdropper and propose a flexible power strategy to enhance the system security. The main contributions of this paper are summarized as follows:

- To the best of the authors, we first fill the internal eavesdropping research gap in existing studies on PA systems. In this paper, we consider a typical NOMA system with two users, where a public information user close to the BS has a potential risk of intercepting the confidential information of user far away from the BS. In the conventional fixed antenna system, due to a better channel condition of the public information user, the confidential information is decoded by the public information user with a high probability. However, PA systems can enhance the channel condition of the far confidential information user while weakening that of the near public user. When public information user's channel condition is no worse than that of the confidential information user, PA systems can enhance the system security by differentiated power allocation, i.e., more power to the PA serving the confidential information user and less power to that for the public information user.
- We analyze the SOP for the PA-aided NOMA systems with internal eavesdropping. We derive exact closed-form expressions for SOP and perform asymptotic analysis to reveal the impact of PA in enhancing the secrecy performance. Since the two conventional power models, i.e., the equal power model and the proportional power model, allocate less or the same power to the PA farther from the BS, they cannot effectively address scenarios with severe security risks. To address this issue, we propose a flexible power strategy, which involves adjusting the radiated power by using a PA with different coupling lengths or altering the coupling lengths between the PAs and the waveguide. We formulate an optimization problem for improving system security by optimizing the coupling length to regulate the radiated power, and the conclusions derived from the solution process can the PA-aided NOMA system to achieve minimum SOP.
- The results shows that: 1) Compared to conventional fixed antennas, in adverse security scenarios where internal

eavesdropping is near BS, PA can significantly enhance system security by adjusting the PA coupling length; 2) In the NOMA system, to guarantee communication of both public information user and confidential information user while preventing confidential information leakage to public information users, an effective strategy is to set the signal power allocation coefficient of confidential information user much lower than that of public information user. On the premise of ensuring no communication outage for public information user, more power is allocated to confidential information user; 3) We define the maximum eavesdropping distance and maximum reliable transmission distance for user activities. As the activity cell of public information user expands, the SOP decreases; whereas as the activity cell of confidential information user expands, the SOP increases.

C. Organization

The remainder of this paper is organized as follows. Section II introduces a two PAs-aided secure NOMA system with a single waveguide and two paired users, i.e., a far confidential information user and a near public information user attempting to eavesdrop on the confidential information. Section III analyzes the performance of the NOMA system achieved by PA, and derives the exact and asymptotic closed-form expressions of SOP to gain useful insights. In Section IV, we propose the flexible power strategy to improve the holistic performance of the system. To guide users in adjusting the antenna coupling length in different scenarios for achieving a secure transmission, an optimization problem based on proposed strategy is formulated. In Section V, the numerical results are presented to verify the accuracy of theoretical analysis and the effectiveness of the proposed strategy. Finally, Section VI concludes the paper and summarizes the key findings.

II. SYSTEM MODEL

A. System Topology

As shown in Fig. 1, we consider a PA-aided NOMA system consisting of a BS, two NOMA users (U_1 and U_2), a dielectric waveguide¹, and two PAs (PA-1 and PA-2). We consider the case that the number of user is equal to that of PA as the users are far apart from each other. Specifically, U_1 is closer to the BS, while U_2 is farther from the BS. Assume that the i -th PA is placed closest to U_i , where $i \in \{1, 2\}$. Among the users, U_1 is a public information user and U_2 is a confidential information user. Both U_1 and U_2 receive the information in accordance with the NOMA protocol and act as regular transceivers in the communication network. Each user is equipped with a single antenna. In practical application scenarios, there is a clear distinction between the

¹Compare to free-space propagation, the power attenuates in waveguide verges on being negligible, e.g., approximately 0.01-0.03 dB/m for a circular copper waveguide at 15 GHz, and 0.1 dB/m at 28 GHz [28]. This study aims to systematically analyze the potential security vulnerabilities of internal eavesdropping in PA-assisted NOMA systems. In follow-up investigations, the influence of waveguide losses on security performance will be integrally incorporated into the analytical framework.

information requirements of two types of users. Users with a demand for confidential information transmission typically focus on scenarios involving the transmission of personal private information (such as identity privacy, and private conversations) or sensitive account information (such as payment passwords and account permission data). By contrast, users who need to receive public information mainly correspond to scenarios of accessing public information that does not involve sensitive data, such as browsing news and watching entertainment videos.

The waveguide is oriented along the x -axis at a height of d . In this paper, we consider a hostile eavesdropping case, where the untrusted user U_1 is closer to the BS, while the confidential information user U_2 is farther from the BS. The untrusted user can be either the near or the far, but we focus on this case because it is in general more challenging². Since multiple users receive the superimposed signal at the same time, confidential information faces a potential risk of being leaked to U_1 . Specifically, U_1 will employ the successive interference cancellation (SIC) technique to decode U_2 's confidential information from the received superimposed signal after successfully decoding its own information. As such, U_1 poses a potential eavesdropping threat to U_2 as an internal eavesdropper of NOMA. Unlike conventional external eavesdroppers, U_1 has a dual identity in the system. On one hand, as a NOMA user operating in accordance with the intended protocol, U_1 's transmission performance needs to be ensured. On the other hand, as an internal user with potential eavesdropping risks, the security issue needs to be tackled to prevent U_1 from successfully intercepting the confidential information of U_2 .

The spatial coordinates of PAs are denoted as $\varphi_i^{pa} = (x_i, 0, d)$, while the positions of the two NOMA users are specified by $u_i = (x_i, y_i, 0)$. The inherent characteristics of PAs allow for dynamic positional adjustment in response to changes in user positions. Specifically, it is assumed that the two NOMA users are uniformly distributed in two square cells, i.e., C_1 with center at $(-D_1, 0, 0)$ and C_2 with center at $(D_2, 0, 0)$, respectively. Both side lengths of C_1 and C_2 are equal to D . Owing to the substantial inter-user distance, the signal strength received by either user from the PA serving the other user is extremely attenuated. Consequently, the deployment of a single PA is insufficient to fulfill the transmission requirements of NOMA. Therefore, each user is paired with one dedicated PA to meet the operational demands of NOMA communications.

B. Signal Model

In the PAs aided NOMA system, the signal received at U_i can be expressed as

$$y_i = \mathbf{h}_i^H \mathbf{s} + w_i, \quad (1)$$

²The conventional power models of PA, namely the equal power model and the proportional power model, allocate more or an equal amount of power to U_1 , which increase the risk of confidential information leakage. Thus, the scenario where the eavesdropper is closer to the BS is more detrimental compared with that where the eavesdropper is far from the BS. This conclusion is further illustrated in the Sections III, IV and V.

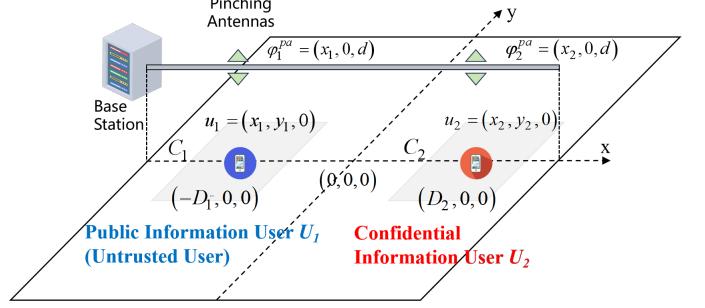


Fig. 1: The two pinching antennas-aided NOMA system, with a single waveguide, a near public information user, and a far confidential information user.

where w_i denotes additive Gaussian noise with zero mean and variance σ^2 . The channel vector can be expressed as [17], [29]

$$\mathbf{h}_i = \left[\frac{\eta^{\frac{1}{2}} e^{-j\frac{2\pi}{\lambda} \|u_i - \varphi_1^{pa}\|}}{\|u_i - \varphi_1^{pa}\|} e^{-j\theta_1}, \frac{\eta^{\frac{1}{2}} e^{-j\frac{2\pi}{\lambda} \|u_i - \varphi_2^{pa}\|}}{\|u_i - \varphi_2^{pa}\|} e^{-j\theta_2} \right]^T, \quad (2)$$

where $\eta = \frac{\lambda^2}{16\pi^2}$ represents the complex channel of the free-space propagation at the reference distance of 1 meter, $\lambda = \frac{c}{f_c}$ denotes the free-space wave length, c is the speed of light, f_c is the carrier frequency, j is the imaginary unit, $\|\cdot\|$ denotes the Euclidean norm, $\theta_i = \frac{2\pi}{\lambda_g} \|\varphi_{bs} - \varphi_i^{pa}\|$ is the phase shift experienced at the i -th PA, $\lambda_g = \lambda/n_{eff}$ is the waveguide wavelength in the dielectric waveguide, n_{eff} is the effective refractive index of a dielectric waveguide, and $\varphi_{bs} = (x_0, 0, d)$ denotes the position of BS.

The two PAs deployed on a single waveguide serve U_1 and U_2 via NOMA technology, and the the superimposed signal s in (1) for the users can be expressed as [25], [30]

$$\mathbf{s} = [\sqrt{p_1}, \sqrt{p_2}]^T (\sqrt{\alpha_1} s_1 + \sqrt{\alpha_2} s_2), \quad (3)$$

where $p_i = P \cdot \epsilon_i$ denotes the transmission power at the i -th PA, P is the transmission power of BS, ϵ_i is the normalized power coefficient of the i -th PA, $s = (\sqrt{\alpha_1} s_1 + \sqrt{\alpha_2} s_2)$ is the superimposed signal, s_i denotes U_i 's signal, α_i denotes the power allocation coefficient for U_i , and $\alpha_1 + \alpha_2 = 1$. According to the coupled-mode theory, ϵ_i can be expressed as [31]

$$\epsilon_i = \begin{cases} F \sin^2(\kappa L_1) & , i = 1, \\ (1 - F \sin^2(\kappa L_1)) F \sin^2(\kappa L_2) & , i = 2, \end{cases} \quad (4)$$

where $0 < F \leq 1$ is the coupling efficiency, κ is the coupling coefficient, and L_i is the coupling length of the i -th PA. Substituting (2) and (3) into (1), the received signal at U_i can be expressed as

$$y_i = \sum_{n=1}^2 p_i \frac{\eta^{\frac{1}{2}} e^{-j\frac{2\pi}{\lambda} \|u_i - \varphi_n^{pa}\|}}{\|u_i - \varphi_n^{pa}\|} e^{-j\theta_n} s + w_i. \quad (5)$$

The channel strength of U_i is denote by $|h_i|^2$, where $h_i = \sum_{n=1}^2 \frac{\eta^{\frac{1}{2}} e^{-j\frac{2\pi}{\lambda} \|u_i - \varphi_n^{pa}\|}}{\|u_i - \varphi_n^{pa}\|} e^{-j\theta_n}$. Since the two users and their corresponding active cells are far apart, large-scale path loss dominates the channel gain, and the distance between U_i and

the PAs becomes the key factor. Moving a PA a few wavelengths to satisfy $\frac{2\pi}{\lambda} \|u_i - \varphi_i^{pa}\| = 2k\pi$ has a limited impact on the distance between PA and user, where k is an arbitrary integer. Therefore, h_i can be simplified as [12]

$$|h_i|^2 = \frac{\eta}{\|u_i - \varphi_i^{pa}\|^2}. \quad (6)$$

Furthermore, given that $D < |D_1 + D_2|$, this condition ensures the two activity cells are separated from each other and have no overlapping areas. In the equal power model, the two PAs deployed on a single waveguide have the same radiated power. Based on this characteristic, the PA-aided NOMA system can be equivalently regarded as two conventional antennas with consistent radiation intensity, and these two antennas are arranged in parallel along the x-axis. This system design enables the establishment of a robust communication link, but it also increases the risk of confidential signals leakage.

To ensure secure transmission, the signal power coefficients are optimized in line with the priority-based NOMA power allocation principle. Specifically, a higher signal power coefficient is assigned to the public information user (prone to eavesdropping), while a lower one is allocated to the user with high security clearance, i.e., $\alpha_1 > \alpha_2$. The core of the SIC technique lies in the sequential decoding process of multi-user signals. First, the system prioritizes and sorts multi-user signals. Then, when a user decodes the target signal, it treats the signals of other users as interference. As such, U_1 treats U_2 's signal as interference and directly decodes its own information. While a less power is allocated to U_2 , and U_2 first decodes U_1 's information successfully. Then, U_2 eliminates the interference from U_1 's signal based on this decoded information, and then decodes its own information. A critical prerequisite for this process is that U_2 obtains U_1 's information to ensure the success of SIC. In this process, the public information user with potential eavesdropping risk attempts to decode the confidential information signal s_2 from the received superimposed signal. The signal-to-interference-plus-noise ratio (SINR) for U_i to decode information signal (s_1 or s_2) is denoted by $\gamma_{u_{i,j}}$, where $i \in \{1, 2\}$ denotes U_1 and U_2 , and $j \in \{1, 2\}$ denotes signal s_1 and s_2 . Based on the above analysis, the SINRs can be expressed as

$$\gamma_{u_{1,1}} = \frac{\alpha_1 \rho_1 |h_1|^2}{\alpha_2 \rho_1 |h_1|^2 + 1}, \quad (7)$$

$$\gamma_{u_{1,2}} = \alpha_2 \rho_1 |h_1|^2, \quad (8)$$

$$\gamma_{u_{2,1}} = \frac{\alpha_1 \rho_2 |h_2|^2}{\alpha_2 \rho_2 |h_2|^2 + 1}, \quad (9)$$

$$\gamma_{u_{2,2}} = \alpha_2 \rho_2 |h_2|^2, \quad (10)$$

where $\rho_i = \rho_t \epsilon_i$ denotes the transmit signal-to-noise ratio (SNR) at the i -th PA, and $\rho_t = \frac{P}{\sigma^2}$ denotes the SNR at the BS.

III. PERFORMANCE ANALYSIS

In this section, we analyze the secrecy performance of the NOMA system achieved by PAs and derive the closed-form SOP. Further, asymptotic analysis is performed to gain deep insights. In particular, a flexible power strategy is proposed

by building upon two conventional power models of PAs. Specifically, by regulating the coupling lengths of PAs, a novel degree of freedom in power allocation is introduced into the PA-aided NOMA system, thereby effectively enhancing the system security.

We define the secrecy outage event of the PA-aided NOMA system as the following three scenarios, where γ_i denotes the minimum decoding SINR threshold of signal s_i .

- U_1 fails to decode the confidential signal s_1 , i.e., $\{\gamma_{u_{1,1}} < \gamma_1\}$.
- U_1 succeeds in eavesdropping on s_2 i.e., $\{\gamma_{u_{1,2}} \geq \gamma_2\}$.
- U_2 fails to decode its own signal s_2 , i.e., $\{\gamma_{u_{2,1}} < \gamma_1 \cup \gamma_{u_{2,2}} < \gamma_2\}$.

Compared with the SOPs in [32], [33], the SOP defined in this work considers two key aspects, i.e., the reliability that both users satisfy the minimum decoding threshold, and the secure transmission requirement of preventing the internal eavesdropper U_1 from decoding s_2 . Therefore, the SOP can be expressed as

$$\begin{aligned} P_{\text{sop}} &= \Pr[\gamma_{u_{1,1}} < \gamma_1 \cup \gamma_{u_{1,2}} \geq \gamma_2 \cup \gamma_{u_{2,1}} < \gamma_1 \cup \gamma_{u_{2,2}} < \gamma_2] \\ &= 1 - \Pr[\gamma_{u_{1,1}} \geq \gamma_1, \gamma_{u_{1,2}} < \gamma_2, \gamma_{u_{2,1}} \geq \gamma_1, \gamma_{u_{2,2}} \geq \gamma_2]. \end{aligned} \quad (11)$$

Substituting (6)–(9) into (11), the SOP is derived as

$$\begin{aligned} P_{\text{sop}} &= 1 - \Pr \left[\frac{\eta \alpha_1 \rho_1 / (y_1^2 + d^2)}{\eta \alpha_2 \rho_1 / (y_1^2 + d^2) + 1} \geq \gamma_1, \frac{\eta \alpha_2 \rho_1}{y_1^2 + d^2} < \gamma_2, \right. \\ &\quad \left. \frac{\eta \alpha_1 \rho_2 / (y_2^2 + d^2)}{\eta \alpha_2 \rho_2 / (y_2^2 + d^2) + 1} \geq \gamma_1, \frac{\eta \alpha_2 \rho_2}{y_2^2 + d^2} \geq \gamma_2 \right] \\ &= 1 - \Pr \left[\frac{\eta \alpha_2 \rho_1}{\gamma_2} - d^2 < y_1^2 \leq \frac{\eta \alpha_1 \rho_1}{\gamma_1} - \eta \alpha_2 \rho_1 - d^2, \right. \\ &\quad \left. y_2^2 \leq \frac{\eta \alpha_1 \rho_2}{\gamma_1} - \eta \alpha_2 \rho_2 - d^2, y_2^2 \leq \frac{\eta \alpha_2 \rho_2}{\gamma_2} - d^2 \right] \\ &= 1 - \Pr[\omega_1 < y_1^2 \leq \omega_2, y_2^2 \leq \min(\omega_3, \omega_4)] \\ &= 1 - \underbrace{\Pr[\omega_1 < y_1^2 \leq \omega_2]}_{\Omega_1} \underbrace{\Pr[y_2^2 \leq \min(\omega_3, \omega_4)]}_{\Omega_2}, \end{aligned} \quad (12)$$

where $\omega_1 = \frac{\eta \alpha_2 \rho_1}{\gamma_2} - d^2$, $\omega_2 = \frac{\eta \alpha_1 \rho_1}{\gamma_1} - \eta \alpha_2 \rho_1 - d^2$, $\omega_3 = \frac{\eta \alpha_1 \rho_2}{\gamma_1} - \eta \alpha_2 \rho_2 - d^2$, $\omega_4 = \frac{\eta \alpha_2 \rho_2}{\gamma_2} - d^2$, Ω_1 denotes the probability that U_1 achieves reliable transmission and the information of U_2 is not leaked, and Ω_2 denotes the probability that U_2 achieves reliable transmission. Both y_1 and y_2 follow a uniform distribution, and their probability density functions (PDFs) are given respectively as

$$f_{Y_1}(y_1) = \begin{cases} \frac{1}{D}, & \text{for } -\frac{D}{2} \leq y_1 \leq \frac{D}{2}, \\ 0, & \text{otherwise.} \end{cases} \quad (13)$$

$$f_{Y_2}(y_2) = \begin{cases} \frac{1}{D}, & \text{for } -\frac{D}{2} \leq y_2 \leq \frac{D}{2}, \\ 0, & \text{otherwise.} \end{cases} \quad (14)$$

Using (13) and (14), the SOP for PAs-aided NOMA systems is presented in the following Lemmas and theorems.

Lemma 1. The exact closed-form expression for Ω_1 in (12)

can be derived as

$$\Omega_1 = \begin{cases} 1, & \omega_1 \leq 0, \omega_2 \geq \frac{D^2}{4}, \\ \frac{2\sqrt{\omega_2}}{D}, & \omega_1 \leq 0, 0 < \omega_2 < \frac{D^2}{4}, \\ \frac{2(\sqrt{\omega_2} - \sqrt{\omega_1})}{D}, & 0 < \omega_1 < \omega_2 < \frac{D^2}{4}, \\ \frac{2(\frac{D}{2} - \sqrt{\omega_1})}{D}, & 0 < \omega_1 < \frac{D^2}{4}, \omega_2 \geq \frac{D^2}{4}, \\ 0, & \text{otherwise.} \end{cases} \quad (15)$$

Proof: See Appendix A. ■

Remark 1. Since Ω_1 represents the probability of ensuring U_1 's reliability while preventing U_2 's information from being intercepted by U_1 , we define $\sqrt{\omega_1}$ as the maximum distance at which U_1 can successfully eavesdrop. When the projection of U_1 's distance from the center of the C_1 on the y-axis is longer than $\sqrt{\omega_1}$, U_1 cannot decode the confidential information of U_2 . We define $\sqrt{\omega_2}$ as the maximum reliable transmission distance for U_1 . The signal s_1 can be decoded by U_1 , when the projection of U_1 's distance from the center of the active area on the y-axis is shorter than $\sqrt{\omega_2}$.

Lemma 2. The expression of Ω_2 in (12) is shown as

$$\Omega_2 = \begin{cases} 1, & \min(\omega_3, \omega_4) \geq \frac{D^2}{4}, \\ \frac{2\sqrt{\min(\omega_3, \omega_4)}}{D}, & 0 < \min(\omega_3, \omega_4) < \frac{D^2}{4}, \\ 0, & \min(\omega_3, \omega_4) \leq 0. \end{cases} \quad (16)$$

Proof: U_2 achieves reliable transmission, i.e., $\Omega_2 = 1$, when the dimensions of U_2 's activity cell is shorter than $\sqrt{\min(\omega_3, \omega_4)}$. The proof of Ω_2 is given by

$$\begin{aligned} \Omega_2 = & \Pr[y_2^2 \leq \min(\omega_3, \omega_4)] \\ = & \frac{1}{D} \left[\mathbb{I}\left(\min(\omega_3, \omega_4) \geq \frac{D^2}{4}\right) \int_{-\frac{D}{2}}^{-\frac{D}{2}} dy_2 \right. \\ & \left. + \mathbb{I}\left(0 < \min(\omega_3, \omega_4) < \frac{D^2}{4}\right) \int_{-\sqrt{\min(\omega_3, \omega_4)}}^{\sqrt{\min(\omega_3, \omega_4)}} dy_2 \right], \end{aligned} \quad (17)$$

where $\mathbb{I}(X)$ denotes the indicator function, which is defined as

$$\mathbb{I}(X) = \begin{cases} 1, & \text{if } X \text{ is true,} \\ 0, & \text{otherwise.} \end{cases} \quad (18)$$

Through mathematical manipulations on (17), we derive the closed-form expressions for Ω_2 as presented in (16), thereby finalizing the proof. ■

Remark 2. From Lemma 2, it can be observed that (16) characterizes the robustness of U_2 's information transmission. Similarly defined to $\sqrt{\omega_2}$, $\sqrt{\min(\omega_3, \omega_4)}$ is defined as the maximum reliable transmission distance for U_2 . When U_i is positioned at the geometric center of C_i , the minimal distance between PAs and users results in enhanced channel. As α_2 is set to be small to ensure U_1 cannot decode s_2 , the system is required to guarantee the successful decoding of s_1 by U_1 and s_2 by U_2 . Consequently, an effective solution is to allocate more power to the far user by adjusting the coupling lengths

Theorem 1. With the helps of Lemmas 1 and 2, the SOP is given by (19), which is shown at the top of the next page.

Proof: The piecewise expressions of Ω_1 and Ω_2 are derived in Lemmas 1 and 2, respectively, with their segmentations determined by the relative magnitudes of $\omega_1, \omega_2, \min(\omega_3, \omega_4)$, and $\frac{D^2}{4}$. The product $\Omega_1 \Omega_2$ is obtained by combining all piecewise conditions of Ω_1 and Ω_2 , followed by substituting their corresponding segment expressions and performing simple algebraic multiplication for each combination. Given the definition $P_{\text{sop}} = 1 - \Omega_1 \Omega_2$, the closed-form expression of P_{sop} in (19) is thereby obtained. Thus, the proof is completed. ■

Remark 3. From Theorem 1, ensuring the reliable transmission of U_1 and U_2 while preventing the leakage of confidential information is the key challenge in the PA-aided NOMA systems. Power allocation is required to satisfy the requirements of all authorized users. At the signal power allocation level, the ratio of α_1 to α_2 needs to exceed the user's decoding threshold, while less power should be allocated to confidential signal s_2 to enhance its security. To further address these issues, at the PA radiated power level, the transmit SNR at PA-1 (ρ_1) can be reduced (while meeting U_1 's decoding threshold) to make $\gamma_{u1,2} < \gamma_2$, and the transmit SNR at PA-2 (ρ_2) can be increased to improve the reliability of U_2 . In conventional fixed antenna-aided NOMA communication systems, when an internal eavesdropper is close to the BS, its channel condition is significantly favorable. This results in NOMA systems with a high risk of confidential information leakage. PAs address this by regulating radiated power through antenna design, enhancing system security at minimal cost.

To obtain further insights, we examine the system's asymptotic characteristics under high transmission SINR, i.e., $\rho_i \rightarrow \infty$.

Corollary 1. The asymptotic analysis of SOP is given by

$$\lim_{\rho_t \rightarrow \infty} P_{\text{sop}} = 1. \quad (20)$$

Proof: As $\rho_t \rightarrow \infty$, both ω_1 and ω_4 approach infinity. Combining this with (15), it follows that $\Omega_1 = 0$. Further, from (16), it is observed that as $\rho_t \rightarrow \infty$, the asymptotic behavior of ω_3 and the corresponding value of Ω_2 are determined by the sign of $\eta \left(\frac{\alpha_1}{\gamma_1} - \alpha_2 \right)$. Specifically, if $\eta \left(\frac{\alpha_1}{\gamma_1} - \alpha_2 \right) > 0$, ω_3 approaches $+\infty$ and $\Omega_2 = 1$; if $\eta \left(\frac{\alpha_1}{\gamma_1} - \alpha_2 \right) < 0$, ω_3 approaches $-\infty$ and $\Omega_2 = 0$; and if $\eta \left(\frac{\alpha_1}{\gamma_1} - \alpha_2 \right) = 0$, $\omega_3 = -d^2$ with $\Omega_2 = 0$. Substituting the aforementioned values of Ω_1 and Ω_2 into (12) completes the proof. ■

Remark 4. To ensure that the signal s_1 can be successfully decoded, the condition $\frac{\alpha_1}{\gamma_1} - \alpha_2 > 0$ is required to be satisfied, i.e., $\frac{\alpha_1}{\alpha_2} > \gamma_1$. The increase of the transmit SNR decreases the security performance of PA-aided NOMA systems.

IV. FLEXIBLE POWER STRATEGY

The equal power model and the proportional power model are the two conventional power model of PA systems. In

$$P_{\text{sop}} = 1 - \begin{cases} 1, & \omega_1 \leq 0, \omega_2 \geq \frac{D^2}{4}, \min(\omega_3, \omega_4) \geq \frac{D^2}{4}, \\ \frac{2\sqrt{\omega_2}}{D}, & \omega_1 \leq 0, 0 < \omega_2 < \frac{D^2}{4}, \min(\omega_3, \omega_4) \geq \frac{D^2}{4}, \\ \frac{2(\sqrt{\omega_2} - \sqrt{\omega_1})}{D}, & 0 < \omega_1 < \omega_2 < \frac{D^2}{4}, \min(\omega_3, \omega_4) \geq \frac{D^2}{4}, \\ \frac{2(\frac{D}{2} - \sqrt{\omega_1})}{D}, & 0 < \omega_1 < \frac{D^2}{4}, \omega_2 > \frac{D^2}{4}, \min(\omega_3, \omega_4) \geq \frac{D^2}{4}, \\ \frac{2\sqrt{\min(\omega_3, \omega_4)}}{D}, & \omega_1 \leq 0, \omega_2 \geq \frac{D^2}{4}, 0 < \min(\omega_3, \omega_4) < \frac{D^2}{4}, \\ \frac{4\sqrt{\omega_2}\sqrt{\min(\omega_3, \omega_4)}}{D^2}, & \omega_1 \leq 0, 0 < \omega_2 < \frac{D^2}{4}, 0 < \min(\omega_3, \omega_4) < \frac{D^2}{4}, \\ \frac{4(\sqrt{\omega_2} - \sqrt{\omega_1})\sqrt{\min(\omega_3, \omega_4)}}{D^2}, & 0 < \omega_1 < \omega_2 < \frac{D^2}{4}, 0 < \min(\omega_3, \omega_4) < \frac{D^2}{4}, \\ \frac{4(\frac{D}{2} - \sqrt{\omega_1})\sqrt{\min(\omega_3, \omega_4)}}{D^2}, & 0 < \omega_1 < \frac{D^2}{4}, \omega_2 > \frac{D^2}{4}, 0 < \min(\omega_3, \omega_4) < \frac{D^2}{4}, \\ 0, & \text{otherwise.} \end{cases} \quad (19)$$

the equal power model, the normalized power coefficients of two PAs are equal and less than or equal to 0.5. This can be easily achieved by designing the PAs with varying coupling lengths using (4). Although this model fully utilizes each antenna, it reduces the design flexibility in terms of antenna radiation power for NOMA system design, retaining only the same superimposed signal power design at the BS as in conventional NOMA. In the proportional power model, each PA is designed with the same coupling length. Consequently, the power emitted by each PA diminishes gradually along the waveguide, with the power radiated by subsequent PAs maintaining a fixed proportional relationship to that of the preceding ones. This characteristic reveals proportional power model cannot satisfy multiple scenarios.

Based on two conventional power models of PA, i.e., the equal power model and the proportional power model, a flexible power strategy is proposed to address the confidential information leakage of the PA-aided NOMA system with internal eavesdropping. Flexible power strategy achieves a precise power regulation, specifically realizing secure and reliable transmission from two dimensions of signal design and antenna radiation to resist potential internal eavesdropping. In the flexible power strategy, p_1 and p_2 are strongly correlated, with $\epsilon_2 = (1 - F \sin^2(\kappa L_1)) \cdot F \sin^2(\kappa L_2)$. In a multi-PA system with a single waveguide, the PA closest to the BS has the highest priority in terms of power allocation. To achieve secure communication, we formulate an optimal coupling length problem to satisfy the minimum SOP, which can be expressed as

$$\mathcal{P}_1 : \min_{L_1, L_2} P_{\text{sop}}(L_1, L_2) \quad (21a)$$

$$\text{s.t. } \frac{\alpha_1}{\alpha_2} > \gamma_1, \quad (21b)$$

$$\min(\omega_3, \omega_4) > 0, \quad (21c)$$

$$\eta \left(\frac{\alpha_1}{\gamma_1} - \alpha_2 \right) > \eta \frac{\alpha_2}{\gamma_2}, \quad (21d)$$

$$0 < L_1, L_2 \leq \frac{\pi}{2\kappa}. \quad (21e)$$

Specifically, constraint (21b) ensures that the stronger signal s_1 can be successfully decoded by users from the superimposed signal. This satisfies the power allocation principle of NOMA.

Constraints (21c) and (21d) guarantee that Ω_1 and Ω_2 in (12) are non-zero. Constraint (21e) defines the upper bounds of the coupling lengths L_1 and L_2 .

Theorem 2. The optimal solution of problem \mathcal{P}_1 can be divided into four cases according to the maximum values of Ω_1 and Ω_2 . Let L_i^{m*} ($m \in \{1, 2, 3, 4\}$) denote the optimal values of L_1 and L_2 along with their corresponding regions for each case m . These are detailed as follows.

a) *Case 1:* When Ω_1 and Ω_2 can reach their maximum of 1, the feasible regions of L_1 and L_2 are given at the top of the next page, where $A = \frac{\eta\alpha_2}{\gamma_2}$, $B = \eta \left(\frac{\alpha_1}{\gamma_1} - \alpha_2 \right)$, and $r = \sin^2(\kappa L_1)$.

b) *Case 2:* When Ω_1 reaches its maximum of 1 and the maximum of Ω_2 is less than 1, the optimal values of L_1 and L_2 are given by

$$L_1^{2*} = \frac{1}{\kappa} \arcsin \left(\sqrt{\frac{d^2 + D^2/4}{BF\rho_t}} \right), \quad (24)$$

$$L_2^{2*} = \frac{\pi}{2\kappa}. \quad (25)$$

c) *Case 3:* When Ω_2 reaches its maximum of 1 and the maximum of Ω_1 is less than 1, the optimal value of L_1 and the feasible region of L_2 are given by

$$L_1^{3*} = \frac{1}{\kappa} \arcsin \left(\sqrt{\frac{d^2 + D^2/4}{BF\rho_t}} \right), \quad (26)$$

$$L_2^{3*} \in \left(\frac{1}{\kappa} \arcsin \left(\sqrt{\frac{d^2 + D^2/4}{\min(A, B) F \rho_t \left(1 - \frac{F(d^2 + D^2/4)}{BF\rho_t} \right)}} \right), \frac{\pi}{2\kappa} \right). \quad (27)$$

d) *Case 4:* When the maximum values of Ω_1 and Ω_1 are less than 1, the optimal values of L_1 and L_2 are given by

$$L_1^{4*} = \frac{1}{\kappa} \arcsin \left(\sqrt{\frac{BF\rho_t - d^2}{2BF^2\rho_t}} \right), \quad (28)$$

$$L_2^{4*} = \frac{\pi}{2\kappa}. \quad (29)$$

Proof: See Appendix B. ■

Remark 5. The optimal values of L_1 in Cases 2 and 3

$$L_1^{1*} \in \left(\frac{1}{\kappa} \arcsin \left(\sqrt{\frac{d^2 + D^2/4}{BF\rho_t}} \right), \frac{1}{\kappa} \arcsin \left(\sqrt{\min \left(\frac{1}{F} \left(1 - \frac{d^2 + D^2/4}{\min(A, B)F\rho_t} \right), 1, \frac{d^2}{AF\rho_t} \right)} \right) \right), \quad (22)$$

$$L_2^{1*} \in \left(\frac{1}{\kappa} \arcsin \left(\sqrt{\frac{d^2 + D^2/4}{\min(A, B)F\rho_t(1-Fr)}} \right), \frac{\pi}{2\kappa} \right). \quad (23)$$

coincide with the lower bound of L_1^{1*} derived for Case 1. Meanwhile, the optimal values of L_2 in Cases 2 and 4 are equivalent to the upper bound of L_2^{2*} , which is $\frac{\pi}{2\kappa}$. In Case 1, feasible regions of L_1 and L_2 are derived. The users can adjust the coupling lengths of PAs with this region to achieve zero outage. In Cases 2, 3, and 4, the optimal values of coupling lengths are derived, respectively. Since the minimum value of SOP may be greater than zero, the secrecy outage event may occur with a non-zero probability.

Remark 6. The equal power model and the proportional power model cannot address the issue of PA-aided NOMA systems. In the equal power model, both PAs radiate the same power. As the channel conditions for both users are identical, the probability of the public information user decoding confidential information is the same as that of the confidential information user. The equal power model exposes the NOMA systems to a high risk of confidential information leakage. In the proportional power model, PA-2 radiates less power, which may not satisfy U_2 's uninterrupted transmission but decreases the security performance of system. To address these issues, the flexible power strategy can allocate the radiation power by adjusting coupling lengths of PA, in which PA-1 radiates less power to public information user U_1 and PA-2 radiates more power to confidential information user U_2 . The proposed flexible power strategy ensures both U_1 and U_2 can decode their own information and simultaneously prevents U_1 from intercepting the confidential information of U_2 .

Remark 7. PA-1 serves the public information user since they are closer to the BS. The remaining waveguide power is radiated to U_2 by PA-2, which is $\rho_t(1-F \sin^2(\kappa L_1))F \sin^2(\kappa L_2)$. By radiating all of the waveguide's power to U_1 , PA-1 can stop U_2 from transmitting. Therefore, PA-1 to service the user of confidential information is a viable deployment for both users and PAs.

V. SIMULATION RESULTS

In this section, we conduct a comprehensive evaluation of the security performance of the PA-aided NOMA system. The simulation results show the accuracy of the theoretical analysis and illustrate the impacts of key parameters. Unless otherwise stated, we set the carrier frequency $f_c = 28$ GHz, the height of waveguide $d = 3$ m, the speed of light $c = 3 \times 10^8$ m/s, the effective refractive index $n_{eff} = 1.4$ [28], and coupling coefficient $\kappa = 100$ m $^{-1}$. The coupling efficiency is fixed at

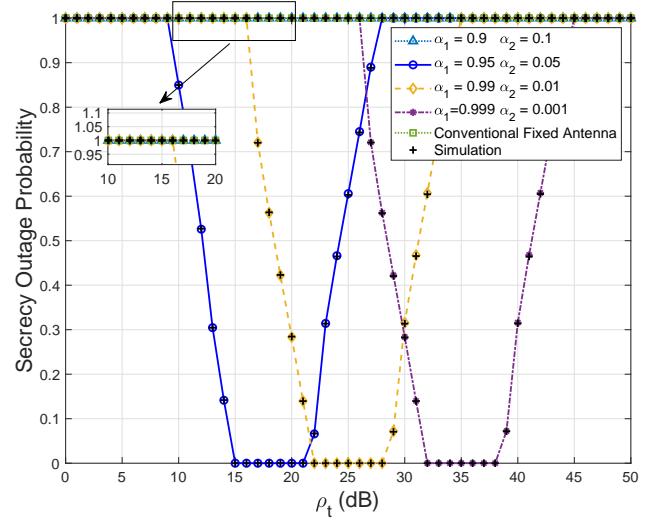


Fig. 2: Secrecy outage probability versus ρ_t for different pairs of signal power allocation coefficients with $L_1 = 1 \times 10^{-3}$ and $L_2 = 1.57 \times 10^{-2}$.

$F = 1^3$, with decoding thresholds $\gamma_1 = 10$ dB and $\gamma_2 = 15$ dB. Additionally, we set the power allocation coefficients $\alpha_1 = 0.01$ and $\alpha_2 = 0.99$, $D_1 = D_2 = 10$ m, and the dimensions of the areas as $D \times D = 10 \times 10$ m 2 . The simulated performance is obtained by performing Monte Carlo simulations over 10^6 realizations.

Fig 2 illustrates the SOP versus transmit SNR ρ_t for different signal power allocation coefficients. It can be observed that the numerical results validate the correctness of the theoretical analysis. The SOP of a conventional fixed antenna-aided NOMA system is considered as a benchmark which shows the superiority of PA-aided NOMA systems in enhancing security. Moreover, as ρ_t increases, the SOP firstly decreases maintains at zero over a certain interval, then increases to 1. However, when $\alpha_1 = 0.9$ and $\alpha_2 = 0.1$, the secrecy outage occurs with the probability of 1. The reason is that the ratio of α_1 to α_2 being lower than γ_1 confirms the conclusion in Remark 4. The decreased α_2 does not improve the security performance of PA-aided NOMA systems, rather, it achieves $P_{sop} = 0$ in the higher SNR range. Because, reducing the value of α_2 decreases the risk of confidential information leakage while increasing the transmission outage probability of

³From the above formulas, it can be inferred that the power emitted by a PA can be regulated by adjusting the coupling length L . When the waveguide and the separate dielectric possess the same effective refractive index, the coupling efficiency F attains its maximum value of 1, enabling the radiation of full power from a single PA with a coupling length of $\pi/(2\kappa)$.

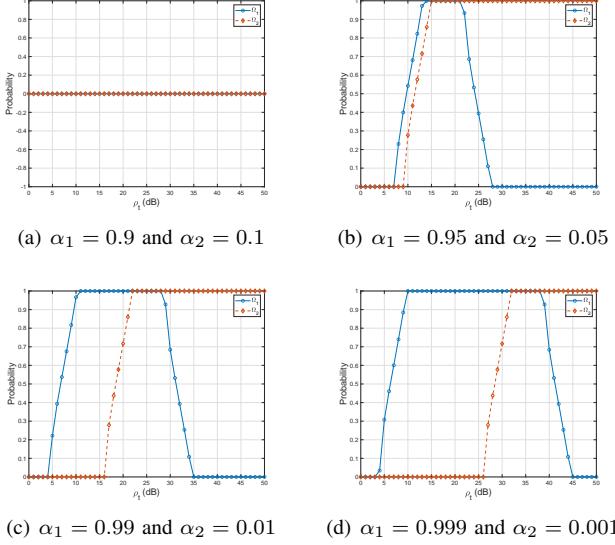


Fig. 3: The probability that U_1 achieves reliable transmission and the information of U_2 is not leaked (Ω_1), and the probability that U_2 achieves reliable transmission (Ω_2) versus transmit SNR ρ_t for different pairs of signal power allocation coefficients with $L_1 = 1 \times 10^{-3}$ and $L_2 = 1.57 \times 10^{-2}$.

U_2 . Additionally, the asymptotic results match the simulation results at high SNR, confirming the accuracy of our asymptotic analysis.

Fig. 3 illustrates the probability (Ω_1) that U_1 achieves a reliable transmission and the information of U_2 is not leaked and the probability (Ω_2) that U_2 achieves a reliable transmission. The increases of Ω_1 and Ω_2 mean the improvement of reliability and security performance of PA-aided NOMA systems. For the curves corresponding to different α_1 and α_2 , the overall trends are similar. Specifically, as ρ_t increases, Ω_1 first rises, maintains at its maximum value of 1 over a certain interval, then decreases to zero. Reducing the value of α_2 expands the range of SNR values over which $\Omega_1 = 1$. This is because security performance is the domain factor with high SNR; the decrease in α_2 increases the difficulty for the public information user to successfully decode s_2 . However, the confidential information user requires a high SNR to decode s_2 with a small power allocation coefficient for s_2 . The SNR required for Ω_2 to reach its maximum value is higher than that for Ω_1 . As SNR increases, Ω_2 begins to rise during the decline phase of Ω_1 , and the peak portions of Ω_1 and Ω_2 do not overlap. This explains why the increase of SNR decreases the SOP achievable by the PA-NOMA system. Simulation results validate the conclusions drawn in Remark 1.

Fig. 4 shows the received SINRs at users. To guarantee the effective decoding of s_1 , the power coefficient ratio $\frac{\alpha_1}{\alpha_2}$ is greater than γ_1 . In the equal power model, users decode the same signals with the same SINRs, i.e., $\gamma_{u_1,1} = \gamma_{u_2,1}$ and $\gamma_{u_2,1} = \gamma_{u_2,2}$. In the proportional power model, the security performance is worse than that in the equal power model, as required for U_2 to decode the confidential information is

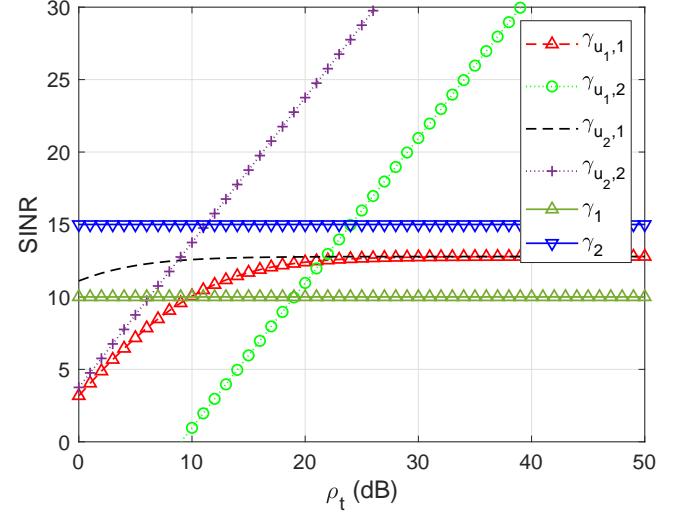


Fig. 4: Signal decoding SINRs of users versus ρ_t with $\alpha_1 = 0.99$, $\alpha_2 = 0.01$, $L_1 = 1 \times 10^{-3}$, and $L_2 = 1.57 \times 10^{-2}$.

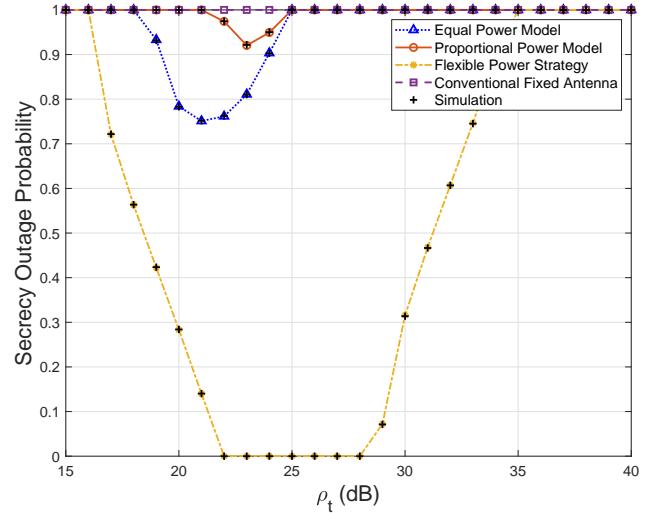
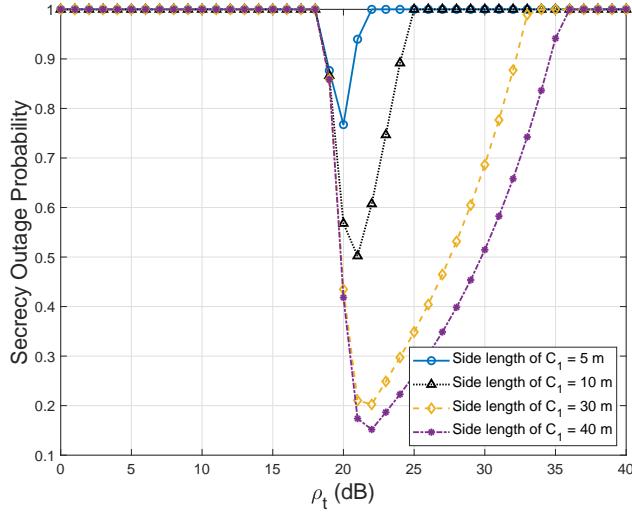


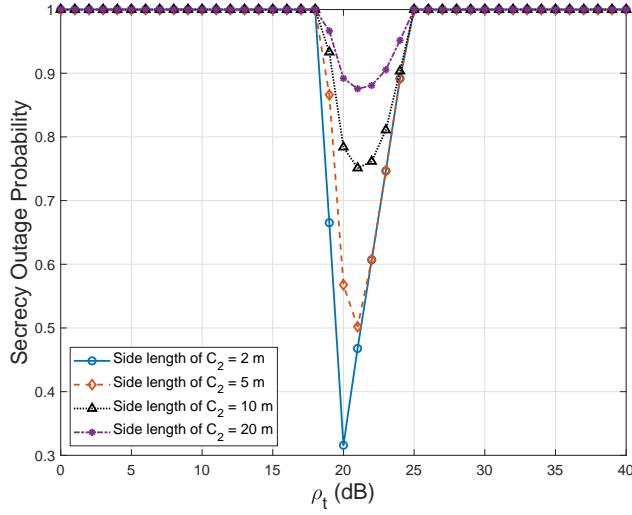
Fig. 5: Comparison among the secrecy outage probability in the flexible power strategy, the secrecy outage probabilities in the equal power model and the proportional power model, and the secrecy outage probability in the conventional fixed antenna aided NOMA system.

lower than that for U_1 . Conventional power models for PA are limited in their ability to improve the security of PA-aided NOMA systems as they cannot adjust the power flexibly. In the flexible power strategy, the PA-aided NOMA systems can adjust the radiated power of PAs increase the SINR required for U_2 to decode the confidential information at low transmit SNR, while decreasing the SINR required for U_1 to decode the confidential information, i.e., $\gamma_{u_1,2} \ll \gamma_{u_2,2}$.

In Fig. 5, the SOP of the PA-aided NOMA system in the flexible power strategy is contrasted with the SOPs of the PA-aided NOMA systems in the two conventional power models and the conventional fixed antenna-aided NOMA system. The results validate the findings in Remarks 3 and 6, demonstrating



(a) The impact of changing the side length of U_1 's activity cell on the SOP with the side length of $C_2 = 10$.



(b) The impact of changing the side length of U_2 's activity cell on the SOP with the side length of $C_1 = 10$.

Fig. 6: Secrecy outage probability versus ρ_t for different side lengths of cells with $\epsilon_1 = \epsilon_2 = 0.5$.

that in the flexible power strategy, PAs fulfill the transmission requirements of both authorized users while reducing the risk of confidential information leakage. When $\rho_t = 21$ dB, the system's SOP in the equal power model reaches a minimum of 0.75 at $L_1 = \frac{\pi}{4\kappa}$ and $L_2 = \frac{\pi}{2\kappa}$. For the proportional power model, we set $L_1 = L_2 = \frac{\pi}{4\kappa}$, where ϵ_2 attains its maximum value of 0.25 and the system achieves a minimum SOP of 0.92 when $\rho_t = 23$. Notably, the conventional power models allocate more (or equal) power to U_1 , which increases the risk of information leaks. In contrast, the flexible power strategy at $L_1 = \frac{\pi}{14\kappa}$ and $L_2 = \frac{\pi}{2\kappa}$ allocates more power to U_2 and less to U_1 , resulting in the SOP remaining at 0 for transmit powers between 22 dB and 28 dB.

Fig. 6(a) illustrates the effect of the side length of C_1 on

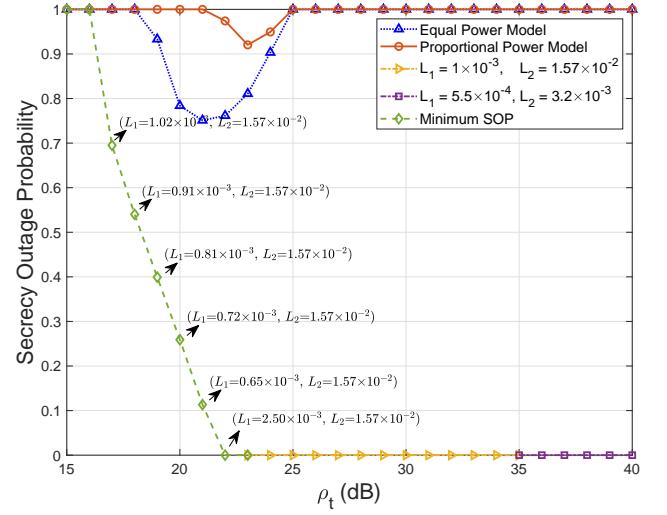


Fig. 7: Secrecy outage probability in the flexible power strategy versus ρ_t .

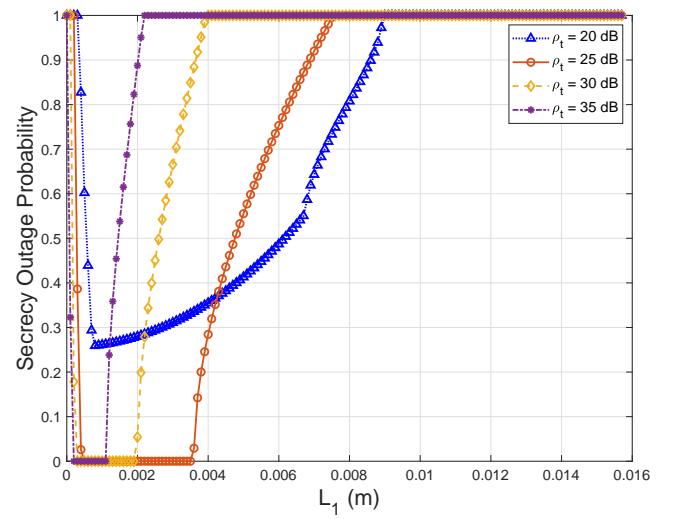


Fig. 8: Secrecy outage probability versus coupling length of PA-1.

the SOP of system. Using the curve for C_1 's side length of 10 as a benchmark, it can be observed that reduction in the public information user's activity cell (C_1) leads to an increase in the SOP. Correspondingly, Fig. 6(b) represents how the side length of C_2 influences the SOP. As C_2 expands, the SOP increases progressively. Specifically, an increase in activity cell leads to a greater distance between the user and the PA, resulting in a decrease in channel strength. Conversely, a smaller activity cell of the public information user increases, the radiated power of the superimposed signal received by the user decreases significantly. Since $\alpha_1 \gg \alpha_2$, U_1 can successfully decode s_1 , but the SINR required for U_1 to decode s_2 is far below the threshold. Consequently, the SOP decreases, and the system security is enhanced. Correspondingly, when the activity cell C_2 increases, the signal power received by U_2

TABLE I: Theoretical vs. simulated coupling length

ρ_t (dB)	Theoretical L_1 (m)	Simulated L_1 (m)	min P_{sop}
17	1.02×10^{-3}	1.1×10^{-3}	0.6950
18	9.1×10^{-34}	1×10^{-3}	0.5401
19	8.1×10^{-4}	9×10^{-4}	0.3993
20	7.25×10^{-4}	8×10^{-4}	0.2590
21	6.46×10^{-4}	7×10^{-4}	0.1133
22	$(5.76 \times 10^{-4}, 2.61 \times 10^{-3})$	$[6 \times 10^{-4}, 2.5 \times 10^{-3}]$	0
23	$(5.13 \times 10^{-4}, 4.58 \times 10^{-3})$	$[6 \times 10^{-4}, 4.5 \times 10^{-3}]$	0

attenuates drastically, preventing the decoding of s_2 . This leads to a decline in the communication reliability of U_2 and, in turn, an increase in the SOP.

Fig. 7 shows the SOPs versus ρ_t under the flexible power strategy. With the help of Theorem 2, we design the optimal values of L_1 and L_2 within the SNR range between 15 dB and 40 dB to achieve the minimum SOP. When the transmit SNR is below 15 dB, the SINR required for U_2 to decode s_2 cannot reach the decoding threshold, thus the SOP remains 0. The simulation results demonstrate that by adjusting the coupling lengths of PA, the flexible power model can satisfy system security requirements under various SNR conditions. The results show that the conventional power models fail to adapt to the dynamic changes of ρ_t . The flexibility of PA is represented in two aspects. On the one hand, dynamic position adjustment can minimize the transmission distance, thereby reducing path loss. On the other hand, precise control of amplification power can enhance system security. It can thus be concluded that the PA-aided NOMA system introduces new degrees of freedom for PLS through the design of normalized power coefficients and the optimized deployment of positions.

Fig. 8 shows the SOPs versus L_1 with $L_2 = 1.57 \times 10^{-2}$ m. Table I shown at the top of the next page presents the coupling lengths through theoretical analysis and simulation when the minimum P_{sop} is achieved with various SNRs. The simulation results verify the accuracy of the theoretical analysis, with errors attributed to limitations in calculation precision and the step size setting during the simulation process. When $17 \leq \rho_t \leq 21$ dB, the minimum value of P_{sop} is greater than 0 as shown in Table I, the maximum value of Ω_1 is 1, and the maximum value of Ω_2 is less than 1. For the other three SNR values, a suitable set of L_1 and L_2 can be found to achieve $P_{\text{sop}} = 0$. The numerical results demonstrate that the proposed optimization scheme can effectively guide the design of PA, thereby improving system security.

VI. CONCLUSION

In this paper, we investigated a PA-aided NOMA system with internal eavesdropping, where the near public information user (U_1) is an internal eavesdropper who eavesdrops on the far confidential information user (U_2). To evaluate the security of the system, we derived the exact closed-form expressions for the SOPs and analyzed the asymptotic behaviors to gain valuable insights. Additionally, to strengthen the security of NOMA systems with internal eavesdroppers, we proposed a flexible power strategy to achieve secure transmission. This

strategy features adaptive power allocation, by optimizing coupling lengths of the PA, it allocates more transmission power to U_2 and less to U_1 . This design specifically addresses the issue that the conventional fixed antenna systems and PA systems (in the equal power model and the proportional power model) have a high risk of confidential information leakage when the internal eavesdropper is near the BS. The results demonstrate that setting small power allocation coefficients to confidential information while allocating more power to the confidential information user via coupling length adjustment is an effective strategy to improve the system's security performance. When the range of the users' activity cells is smaller than the maximum reliable transmission distance, while the range of the eavesdropper's activity cell exceeds the maximum eavesdropping distance, the PA-aided NOMA system can effectively mitigate the risk of confidential information leakage.

APPENDIX A PROOF OF LEMMA 1

To derive the closed-form expressions of Ω_1 in (15), we consider the relationship between feasible range of y_1^2 , i.e., $0 \leq y_1^2 \leq \frac{D^2}{4}$ and the magnitudes of ω_1 and ω_2 . The proof of Ω_1 is given by

$$\begin{aligned} \Omega_1 = & \Pr [\omega_1 < y_1^2 \leq \omega_2] \\ = & \frac{1}{D} \left[\mathbb{I} \left(\omega_1 \leq 0, \omega_2 \geq \frac{D^2}{4} \right) \int_{-\frac{D}{2}}^{\frac{D}{2}} dy_2 \right. \\ & + \mathbb{I} \left(\omega_1 \leq 0, 0 < \omega_2 < \frac{D^2}{4} \right) \int_{-\sqrt{\omega_2}}^{\sqrt{\omega_2}} dy_2 \\ & + \mathbb{I} \left(0 < \omega_1 < \omega_2 < \frac{D^2}{4} \right) \left(\int_{-\sqrt{\omega_2}}^{-\sqrt{\omega_1}} dy_1 + \int_{\sqrt{\omega_1}}^{\sqrt{\omega_2}} dy_1 \right) \\ & \left. + \mathbb{I} \left(0 < \omega_1 < \frac{D^2}{4}, \omega_2 \geq \frac{D^2}{4} \right) \left(\int_{-\frac{D}{2}}^{-\sqrt{\omega_1}} dy_1 + \int_{\sqrt{\omega_1}}^{\frac{D}{2}} dy_1 \right) \right]. \end{aligned} \quad (30)$$

By performing algebraic transformations on (30), we derive Ω_1 as shown in (15), thus completing the proof.

APPENDIX B PROOF OF THEOREM 2

According to (12), the optimization problem \mathcal{P}_1 in (21a) aimed at minimizing SOP is equivalent to maximizing Ω_1 .

Ω_2 the probability of the valid secure transmission event. The equivalent relation is given by

$$\min P_{\text{sop}} \Leftrightarrow \max \Pr[\varepsilon], \quad (31)$$

where $\varepsilon = \{\omega_1 < y_1^2 \leq \omega_2, y_2^2 \leq \min(\omega_3, \omega_4)\}$ denotes the event that U_1 decodes s_1 successfully but fails to decode s_2 , and U_2 decodes both s_1 and s_2 successfully. Since the maximum value of $\Pr[\varepsilon]$ is not guaranteed to be 1, we denote its maximum value as $M \in (0, 1]$. Based on the former analysis of (15) (16), the feasible region for L_1 and L_2 are divided into four cases. Notably, let $r = \sin^2(\kappa L_1)$ and $t = \sin^2(\kappa L_2)$. Let r^{j*} and t^{j*} denote the corresponding optimal values of r and t in different cases, respectively.

a) *Case 1:* The maximum values of Ω_1 and Ω_2 reach 1. From (15), the maximum value $\Omega_1 = 1$ holds if and only if $\omega_1 \leq 0$ and $\omega_2 \geq \frac{D^2}{4}$, which is equivalent to the following relations:

$$\begin{cases} AF\rho_t r^{1*} - d^2 \leq 0, \\ BF\rho_t r^{1*} - d^2 \geq \frac{D^2}{4}. \end{cases} \quad (32)$$

After performing mathematical transformations on the above formulas, we obtain the range of r^{1*} as

$$\frac{d^2 + D^2/4}{BF\rho_t} \leq r^{1*} \leq \min\left(1, \frac{d^2}{A\rho_t F}\right). \quad (33)$$

From (16), Ω_2 obtains the maximum value of 1 if and only if $\min(\omega_3, \omega_4) \geq \frac{D^2}{4}$. This is equivalent to

$$\min\left(\eta\left(\frac{\alpha_1}{\gamma_1} - \alpha_2\right), \eta\frac{\alpha_2}{\gamma_2}\right) F\rho_t (1 - Fr^{1*}) t^{1*} - d^2 \geq \frac{D^2}{4}. \quad (34)$$

We can obtain the co-relationship of r^{1*} and t^{1*} as

$$\frac{d^2 + D^2/4}{\min(A, B)F\rho_t (1 - Fr^{1*})} \leq t^{1*} \leq 1. \quad (35)$$

Since $t^{1*} \in (0, 1]$, The upper bound of r^{1*} is derived as

$$(1 - Fr^{1*}) \geq \frac{d^2 + D^2/4}{\min(A, B)F\rho_t} \Rightarrow r^{1*} \leq \frac{1}{F} \left(1 - \frac{d^2 + D^2/4}{\min(A, B)F\rho_t}\right). \quad (36)$$

Combining (33) and (36), the effective range of r is written as

$$\frac{d^2 + D^2/4}{BF\rho_t} \leq r^{1*} \leq \min\left(\frac{1}{F} \left(1 - \frac{d^2 + D^2/4}{\min(A, B)F\rho_t}\right), 1, \frac{d^2}{A\rho_t F}\right), \quad (37)$$

where $r = 1$, i.e., $L_1 = \frac{\pi}{2\kappa}$ is allowed only if $1 - Fs \neq 0$. Since $r = \sin^2(\kappa L_1)$ is monotonically increasing for $L_1 \in (0, \frac{\pi}{2\kappa}]$, the feasible region of L_1 is obtained by inverting r^{1*} via $L_1^{1*} = \frac{1}{\kappa} \arcsin(\sqrt{r^{1*}})$. After fixing L_1^{1*} , substituting L_1^{1*} into (35) and using the monotonicity of $t = \sin^2(\kappa L_2)$, the feasible region of L_2^{1*} is derived similarly.

b) *Case 2:* Only Ω_1 reaches its maximum of 1. In order to obtain the minimum value of P_{sop} , we first analyze the monotonic relationship of Ω_2 with respect to r^{2*} and t^{2*} as

$$\Omega_2 \propto \frac{2}{D} \sqrt{\min(\omega_3, \omega_4)} = \min(B, A) F\rho_t (1 - Fr^{2*}) t^{2*}. \quad (38)$$

Since Ω_2 is monotonically increasing with t , we set $L_2^{2*} = \frac{\pi}{2\kappa}$. With $L_2 = L_2^{2*}$, problem \mathcal{P}_1 reduces to a single-variable optimization over r^{2*} , i.e., L_1^{2*} , where the objective function is written as

$$\min P_{\text{sop}} \Leftrightarrow \max f(r^{2*}) = \Omega_1(r^{2*}) \cdot (1 - Fr^{2*}), \quad (39)$$

where $1 - Fr$ denotes the residual power ratio in the waveguide after PA-1 radiates power. When $\Omega_1(r^{2*}) = 1$, i.e., $r^{2*} \geq \frac{d^2 + D^2/4}{BF\rho_t}$, $f(r^{2*}) = 1 \cdot (1 - Fr^{2*})$, which is monotonically decreasing with r . Thus, the optimal s is the minimum value that satisfies $\Omega_1(r^{2*}) = 1$, i.e., $r^{2*} = \frac{d^2 + D^2/4}{BF\rho_t}$. The corresponding optimal L_1 is given by

$$L_1^{2*} = \frac{1}{\kappa} \arcsin\left(\sqrt{\frac{d^2 + D^2/4}{BF\rho_t}}\right). \quad (40)$$

c) *Case 3:* Only Ω_2 reaches its maximum of 1. Similarly, the monotonicity of Ω_1 with respect to r^{3*} is analyzed as

$$\Omega_1 \propto |\omega_2 - \omega_1| = (B - A) F\rho_t r^{3*}, \quad (41)$$

where $\omega_1 \geq 0, \omega_2 \leq \frac{D^2}{4}$, the feasible region of r^{3*} is given as

$$\frac{d^2}{AF\rho_t} \leq r^{3*} \leq \frac{d^2 + D^2/4}{BF\rho_t}. \quad (42)$$

Since P_{sop} is monotonicity decreasing with r^{3*} , the optimal value of r^{3*} is $\frac{d^2 + D^2/4}{BF\rho_t}$, and the feasible region of t is given as

$$\frac{d^2 + D^2/4}{\min(A, B) F\rho_t \left(1 - \frac{F(d^2 + D^2/4)}{BF\rho_t}\right)} \leq t^{3*} \leq 1. \quad (43)$$

Through algebraic manipulations on r^{3*} and t^{3*} , the proof of case 3 is completed.

d) *Case 4:* The maximum values of Ω_1 and Ω_2 are less than 1. We consider the situation that $0 < \omega_1 < \omega_2 < \frac{D^2}{4}$. Based on the monotonicity analysis of Ω_1 and Ω_2 presents in (41) and (38), $f(r^{4*})$ is written as

$$f(r^{4*}) = \frac{2}{D} (\sqrt{\omega_2} - \sqrt{\omega_1}) \cdot \Omega_2(r^{4*}, 1). \quad (44)$$

Since $B > A$, $\Omega_2(r, 1) = \frac{2}{D} \sqrt{\omega_3}$. $f(r^{4*})$ can be given by

$$f(r^{4*}) = \frac{D^2}{4} \left(\sqrt{BF\rho_t r^{4*} - d^2} - \sqrt{AF\rho_t r^{4*} - d^2} \right) \times \sqrt{BF\rho_t r^{4*} (1 - Fr^{4*}) - d^2}. \quad (45)$$

Maximizing $f(r^{4*})$ is equivalent to maximizing its square, given that the range of $f(r^{4*})$ is non-negative, i.e., $f(r^{4*}) \geq 0$ for all s in the domain. We thus define an auxiliary function $g(r^{4*})$ as the square of $f(r^{4*})$, i.e., $g(r^{4*}) = [f(r^{4*})]^2$. We differentiate $g(r^{4*})$ with respect to r^{4*} and set the derivative to zero as

$$\frac{dg(r^{4*})}{dr^{4*}} \propto u'(r^{4*})v(r^{4*}) + u(r^{4*})v'(r^{4*}), \quad (46)$$

$$\begin{aligned} u(r^{4*}) &= \left(\sqrt{BF\rho_t r^{4*} - d^2} - \sqrt{AF\rho_t r^{4*} - d^2} \right)^2, \\ v(r^{4*}) &= BF\rho_t (1 - Fr^{4*}) - d^2, \\ u'(r^{4*}) &= \left(\sqrt{BF\rho_t r^{4*} - d^2} - \sqrt{AF\rho_t r^{4*} - d^2} \right) \end{aligned}$$

$$\times \left(\frac{BF\rho_t}{\sqrt{BF\rho_t r^{4*} - d^2}} - \frac{AF\rho_t}{\sqrt{AF\rho_t r^{4*} - d^2}} \right), \quad \text{and} \quad v'(r^{4*}) = -BF^2\rho_t^{4*}.$$

To obtain an approximate solution, we further assume that ω_1 and ω_2 are much greater than 0. Correspondingly, $f(r^{4*})$ can be approximated as

$$f(r^{4*}) \approx \frac{4}{D^2} \sqrt{r^{4*}} \left(\sqrt{BF\rho_t} - \sqrt{AF\rho_t} \right) \times \sqrt{BF\rho_t(1 - Fr^{4*}) - d^2}, \quad (47)$$

which attains its extremum when $r^{4*} = \frac{BF\rho_t - d^2}{2BF^2\rho_t}$. Since there is no elementary analytical solution, we first determine the feasible interval of r^{4*} as $r^{4*} \in \left(\frac{d^2}{AF\rho_t}, \min \left(\frac{d^2 + D^2/4}{BF\rho_t}, \frac{BF\rho_t - d^2}{BF\rho_t^2}, 1 \right) \right)$, and then solve for the optimal solution using the bisection method. The proof is completed.

REFERENCES

- [1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, May 2020.
- [2] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6G: Visions, requirements, key technologies, and testbeds," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 905–974, Secondquarter 2023.
- [3] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, Jan. 2020.
- [4] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948.
- [5] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.
- [6] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2283–2314, Fourthquarter 2020.
- [7] C. Huang, A. Zappone, G. C. Alexandopoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.
- [8] K.-K. Wong, A. Shojaeifard, K.-F. Tong, and Y. Zhang, "Fluid antenna systems," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1950–1962, Mar. 2021.
- [9] L. Zhu, W. Ma, and R. Zhang, "Modeling and performance analysis for movable antenna enabled wireless communications," *IEEE Transactions on Wireless Communications*, vol. 23, no. 6, pp. 6234–6250, Jun. 2024.
- [10] J. Chen, K. Cao, P. D. Diamantoulakis, L. Lv, L. Yang, H. Chi, and H. Ding, "Secure wireless-powered zeRIS communications," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2025, early access.
- [11] Z. Yang, N. Wang, Y. Sun, Z. Ding, R. Schober, G. K. Karagiannidis, V. W. Wong, and O. A. Dobre, "Pinching antennas: Principles, applications and challenges," *IEEE Wireless Communications*, pp. 1–10, 2025, early access.
- [12] X. Xie, F. Fang, Z. Ding, and X. Wang, "A low-complexity placement design of pinching-antenna systems," *IEEE Communications Letters*, vol. 29, no. 8, pp. 1784–1788, Aug. 2025.
- [13] M. Sun, C. Ouyang, S. Wu, and Y. Liu, "Physical layer security for pinching-antenna systems (PASS)," Mar. 2025. [Online]. Available: <http://arxiv.org/abs/2503.09075>
- [14] H. O. Y. Suzuki and K. Kawai, "Pinching antenna-using a dielectric waveguide as an antenna," *NTT DOCOMO Technical Journal*, vol. 23, no. 3, pp. 5–12, Jan. 2022.
- [15] Y. Liu, Z. Wang, X. Mu, C. Ouyang, X. Xu, and Z. Ding, "Pinching-antenna systems: Architecture designs, opportunities, and outlook," *IEEE Communications Magazine*, pp. 1–7, 2025, early access.
- [16] J. Guo, Y. Liu, and A. Nallanathan, "A graph neural network for learning beamforming in pinching antenna systems (PASS)," *IEEE Wireless Communications Letters*, pp. 1–1, 2025, early access.
- [17] Z. Ding, R. Schober, and H. Vincent Poor, "Flexible-antenna systems: A pinching-antenna perspective," *IEEE Transactions on Communications*, vol. 73, no. 10, pp. 9236–9253, Oct. 2025.
- [18] C. Ouyang, Z. Wang, Y. Liu, and Z. Ding, "Array gain for pinching-antenna systems (PASS)," *IEEE Communications Letters*, vol. 29, no. 6, pp. 1471–1475, Jun. 2025.
- [19] D. Tyrovolas, S. A. Tegos, P. D. Diamantoulakis, S. Ioannidis, C. K. Liaskos, and G. K. Karagiannidis, "Performance analysis of pinching-antenna systems," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2025, early access.
- [20] S. A. Tegos, P. D. Diamantoulakis, Z. Ding, and G. K. Karagiannidis, "Minimum data rate maximization for uplink pinching-antenna systems," *IEEE Wireless Communications Letters*, vol. 14, no. 5, pp. 1516–1520, May 2025.
- [21] T. Hou, Y. Liu, and A. Nallanathan, "On the performance of uplink pinching antenna systems (PASS)," *IEEE Transactions on Communications*, pp. 1–1, 2025, ealy access.
- [22] S. Lv, Y. Liu, and Z. Ding, "Beam training for pinching-antenna systems (PASS)," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2025, early access.
- [23] A. Bereyhi, S. Asaad, C. Ouyang, Z. Ding, and H. V. Poor, "Downlink beamforming with pinching-antenna assisted MIMO systems," in *2025 IEEE International Conference on Communications Workshops (ICC Workshops)*, Jun. 2025, pp. 1–6.
- [24] Z. Wang, C. Ouyang, X. Mu, Y. Liu, and Z. Ding, "Modeling and beam-forming optimization for pinching-antenna systems," *IEEE Transactions on Communications*, pp. 1–1, 2025, early access.
- [25] K. Wang, Z. Ding, and R. Schober, "Antenna activation for NOMA assisted pinching-antenna systems," *IEEE Wireless Communications Letters*, vol. 14, no. 5, pp. 1526–1530, May 2025.
- [26] Y. Fu, F. He, Z. Shi, and H. Zhang, "Power minimization for NOMA-assisted pinching antenna systems with multiple waveguides," Mar. 2025, arXiv:2503.20336 [cs]. [Online]. Available: <http://arxiv.org/abs/2503.20336>
- [27] O. S. Badarneh, H. S. Silva, and Y. H. A. Badarneh, "Physical-Layer Security of Pinching-Antenna Systems," Mar. 2025, arXiv:2503.18322 [cs]. [Online]. Available: <http://arxiv.org/abs/2503.18322>
- [28] D. M. Pozar, *Microwave Engineering*, 4th ed. New York, US: John Wiley & Sons, 2011.
- [29] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, M. F. Imani, and Y. C. Eldar, "Beam focusing for near-field multiuser MIMO communications," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7476–7490, Sept. 2022.
- [30] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-s. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 721–742, Secondquarter 2017.
- [31] K. Okamoto, *Fundamentals of Optical Waveguides*. San Diego, CA, USA: Elsevier, 2006.
- [32] J. Chen, K. Cao, H. Ding, L. Lv, Y. Ye, H. Chi, T. Wang, and L. Yang, "Double-RIS enabled physical layer security for wireless-powered communication systems over rayleigh fading channels," *IEEE Transactions on Communications*, vol. 73, no. 10, pp. 9517–9535, Oct. 2025.
- [33] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA s systems against internal and external eavesdropping," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2930–2943, 2020.