Computer Communications 242 (2025) 108274

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Physical layer security in FAS-aided wireless powered NOMA systems☆

Farshad Rostami Ghadi [a,1], Masoud Kaveh [c,1], Kai-Kit Wong [a,b,2], Diego Martín [d,*], Riku Jäntti [c,3], Zheng Yan [e,2]

[a] Department of Electronic and Electrical Engineering, University College London, London, UK
[b] Department of Electronic Engineering, Kyung Hee University, Yongin-si, Gyeonggi-do 17104, Republic of Korea
[c] Department of Information and Communication Engineering, Aalto University, 02150 Espoo, Finland
[d] Department of Computer Science, Escuela de Ingeniería Informática de Segovia, Universidad de Valladolid, Segovia, 40005, Spain
[e] School of Cyber Engineering Xidian University, Xi'an, China

ARTICLE INFO

Keywords:
Wireless powered communication network
Fluid antenna system
Physical layer security
Non-orthogonal multiple access
Secrecy outage probability
Average secrecy capacity

ABSTRACT

The rapid evolution of communication technologies and the emergence of sixth-generation (6G) networks have introduced unprecedented opportunities for ultra-reliable, low-latency, and energy-efficient communication. Integrating technologies like non-orthogonal multiple access (NOMA) and wireless powered communication networks (WPCNs) brings new challenges. These include energy constraints and increased security vulnerabilities. Traditional antenna systems and orthogonal multiple access schemes struggle to meet the increasing demands for performance and security in such environments. To address this gap, this paper investigates the impact of emerging fluid antenna systems (FAS) on the performance of physical layer security (PLS) in WPCNs. Specifically, we consider a scenario in which a transmitter, powered by a power beacon via an energy link, transmits confidential messages to legitimate FAS-aided users over information links while an external eavesdropper attempts to decode the transmitted signals. Additionally, users leverage the NOMA scheme, where the far user may also act as an internal eavesdropper. For the proposed model, we first derive the distributions of the equivalent channels at each node and subsequently obtain compact expressions for the secrecy outage probability (SOP) and average secrecy capacity (ASC), using the Gaussian quadrature methods. Our results reveal that incorporating the FAS for NOMA users, instead of the TAS, enhances the performance of the proposed secure WPCN.

1. Introduction

The rapid advancements in communication technologies and the emergence of the sixth generation (6G) network promise unprecedented capabilities, including ultra-high data rates, massive connectivity, and near-zero latency. However, these advances come with significant energy challenges, particularly for devices that are energy-constrained [1]. In 6G networks, the densification of base stations, the proliferation of edge devices, and the continuous demand for high-speed communication place tremendous strain on energy resources. Traditional battery powered devices face inherent limitations, such as frequent recharging, short operating lifetimes, and the environmental impact of large-scale battery production and disposal [2]. These constraints threaten the feasibility of deploying energy-efficient and sustainable networks on the scale envisioned for 6G.

To overcome these challenges, innovative solutions are required to ensure reliable and perpetual operation of devices without reliance on conventional battery technologies. wireless powered communication networks (WPCNs) have emerged as a promising solution by integrating

☆ The work of F. R. Ghadi and K. K. Wong is supported by the Engineering and Physical Sciences Research Council (EPSRC), United Kingdom under Grant EP/W026813/1. The work of M. Kaveh and R. Jäntti has received funding from the SNS JU under the EU's Horizon Europe research and innovation programme under Grant Agreement No. 101192113. The work of D. Martín has been developed within the project PRESECREL (PID2021-124502OB-C43). We would like to acknowledge the financial support of the Ministerio de Ciencia e Investigación, (Spain), in relation to the Plan Estatal de Investigación Científica y Técnica y de Innovación 2017–2020.

* Corresponding author.
E-mail addresses: f.rostamighadi@ucl.ac.uk (F. Rostami Ghadi), masoud.kaveh@aalto.fi (M. Kaveh), kai-kit.wong@ucl.ac.uk (K.-K. Wong), diego.martin.andres@uva.es (D. Martín), riku.jantti@aalto.fi (R. Jäntti), zyan@xidian.edu.cn (Z. Yan).
[1] Member, IEEE.
[2] Fellow, IEEE.
[3] Senior Member, IEEE.

https://doi.org/10.1016/j.comcom.2025.108274
Received 15 January 2025; Received in revised form 19 May 2025; Accepted 6 July 2025
Available online 19 July 2025

wireless power transfer (WPT) with communication systems [3–5]. WPCNs enable energy-constrained devices to harvest energy wirelessly while maintaining data communication, thus eliminating the dependence on batteries for continuous operation [6]. This approach is particularly well suited to support the demands of 6G networks, where scalability, sustainability, and uninterrupted connectivity are paramount. By combining energy transfer with data communication, WPCNs offer a sustainable and efficient framework to support a wide range of energy-constrained applications, such as the Internet of Things (IoT) [7–9], backscatter communication (BC) [10–13], sensor networks [14], smart grids [15,16], vehicle-to-vehicle (V2V) [17], and remote monitoring systems [18].

On the other hand, multi-input multi-output (MIMO) systems face challenges such as high complexity in hardware and signal processing, limited spatial diversity in compact devices, and performance degradation in dynamic environments with poor channel conditions [19]. Fluid antenna systems (FASs) have shown promising potential to address these by dynamically adapting antenna positions to optimize signal reception, enabling higher diversity gains and better performance in fluctuating environments, while reducing the complexity associated with traditional multi-antenna setups [20–22]. FAS leverages fluidic or dielectric structures that are software-manageable, allowing the antenna to dynamically modify its shape, position, and configuration to optimize radiation characteristics [23–26]. This unique feature, which sets FAS apart from traditional antenna systems (TASs), is made possible by advancements in liquid-metal technologies and RF-switchable pixels. The integration of FASs into WPCNs presents a transformative opportunity to enhance the adaptability and efficiency of these networks [27]. These innovations allow FAS to outperform TAS by enhancing energy efficiency and improving the reliability of data transmission in WPCNs [28,29]. In the context of WPCNs, FAS enables real-time adaptation to varying channel conditions, ensuring optimal energy harvesting and information transfer in challenging environments, such as those with high mobility or severe multipath fading. By dynamically selecting the optimal antenna configuration based on channel state information (CSI), FAS minimizes energy wastage, maximizes transmission reliability, and ensures uninterrupted operation [30]. This capability is perfectly in line with the energy efficient and sustainable design principles of WPCNs, making FAS particularly valuable for applications in IoT, smart city infrastructures, and remote monitoring systems.

To clearly establish the paper's focus, this work (i) introduces a secure WPCN framework that combines FAS with a modern multiple access technique under energy harvesting, considering two distinct eavesdropping scenarios; (ii) presents closed-form secrecy performance metrics based on a compact analytical formulation; and (iii) validates the proposed model through simulations that examine the impact of FAS on communication secrecy.

1.1. Related works

Physical layer security (PLS) has gained significant attention in WPCNs due to its potential to protect sensitive information. Several works have explored challenges and solutions in this domain. Jiang et al. [31] analyzed the secrecy performance of wirelessly powered wiretap channels, where an energy-constrained multi-antenna source, powered by a dedicated power beacon (PB), communicates in the presence of a passive eavesdropper. They proposed time-switching protocols and evaluated maximum ratio transmission and transmit antenna selection schemes. Their results demonstrated the critical role of full CSI in achieving substantial secrecy diversity gain and highlighted that wireless power transfer randomness does not degrade secrecy performance in high signal-to-noise ratio (SNR) regimes. Huang et al. [32] studied the secrecy performance in wireless communication networks powered by multiple eavesdroppers. They considered the maximum ratio transmission and transmit antenna selection schemes under both non-colluding and colluding eavesdroppers. Closed-form expressions for secrecy outage probability (SOP) and average secrecy capacity (ASC) were derived, showing that feedback delay significantly impacts secrecy diversity. Their findings indicate that the transmit antenna selection scheme performs comparably or even better than the maximum ratio transmission under moderate feedback delays. Cao et al. [33] explored PLS in reconfigurable intelligent surfaces (RIS)-aided WPCNs for IoT. They proposed three RIS-aided secure WPC modes, optimizing IRS phase shifts to enhance energy and information transfer. Their analysis revealed that mode-I achieves the best connection outage probability (COP), mode-II the best SOP, and mode-II outperforms others in ASC with higher transmission power or RIS elements, demonstrating the critical role of IRS configurations in balancing reliability and security.

FASs have emerged as transformative technologies for improving PLS, with several studies exploring its potential in enhancing secure communication under diverse scenarios. The authors in [34] investigated the PLS performance of FAS-aided communication systems over arbitrary correlated fading channels. They derived analytical expressions for secrecy metrics, such as ASC, SOP, and secrecy energy efficiency (SEE), using Gaussian copulas and Gauss–Laguerre quadrature. Their findings demonstrated that FAS with a single activated port outperforms TASs, such as maximal ratio combining (MRC) and antenna selection (AS), in secure transmission reliability. Vega-Sánchez et al. [35] analyzed the SOP of FAS in systems experiencing spatially correlated Nakagami-m fading. They compared non-diversity FAS and maximum-gain combining FAS (MGC-FAS) against multiple antennas with MRC at the eavesdropper. Their closed-form approximations revealed that MGC-FAS achieves superior secrecy performance when the FAS tube's size is sufficiently large and the legitimate path's average SNR significantly exceeds the eavesdropper's link SNR. The authors in [36] explored the integration of RIS with FAS for secure communications in wiretap scenarios. Their analysis focused on deriving the cumulative distribution function (CDF) and probability density function (PDF) of the SNR at each node using Gaussian copulas, leading to compact expressions for the SOP. The results demonstrated that the combination of FAS with RIS substantially enhances secure communication performance, underscoring the synergy between these technologies in next-generation networks.

Most existing studies on FAS integration have predominantly focused on the use of orthogonal multiple access (OMA) schemes. Although OMA has been widely adopted because of its simplicity, it is not the most efficient approach when the CSI at the transmitter is known. In this regard, several studies have demonstrated the significant advantages of the NOMA principle over OMA in FAS [37–39]. Using superposition coding and successive interference cancellation (SIC), NOMA allows multiple users to share the same frequency resources, improving spectral efficiency and system performance. Therefore, highlighting the advantages of NOMA in FAS, the authors in [27] integrated WPCN with FAS under a NOMA scenario, demonstrating how FAS outperforms TAS for both near and far users in the WPCN.

1.2. Motivations and contributions

While various combinations of FAS, WPCNs, NOMA, and PLS have been individually studied in prior research, their simultaneous integration for secure communication remains unexplored. The potential synergy of combining FAS with NOMA-enabled WPCNs to enhance PLS presents a promising yet unresolved research question. As these systems become increasingly critical to next-generation networks, ensuring their security is of utmost importance. However, their unique structure introduces distinct vulnerabilities that demand dedicated attention. Therefore, building on the work in [27], we propose extending the system to a secure communication framework by combining FAS with NOMA-enabled WPCNs. This scenario potentially involves two eavesdropping models: (i) an external eavesdropper positioned between legitimate users, attempting to intercept transmissions, and (ii)

a far NOMA user acting as an internal eavesdropper, exploiting shared resources to compromise communication secrecy. In this regard, we analyze the secrecy performance of both the external and internal eavesdropping scenarios, deriving a compact analytical framework of key secrecy metrics such as SOP and ASC. The main contributions of this paper are summarized as follows:

- We propose a novel FAS-aided WPCN framework that integrates energy efficiency with secure transmission under the NOMA scheme, introducing two eavesdropping scenarios: external and internal.
- For both eavesdropping scenarios, we first derive the CDF and PDF of the equivalent channel gain for each FAS-equipped NOMA user in terms of the multivariate normal distribution. Subsequently, we obtain compact analytical expressions for the SOP and ASC of both users under external and internal eavesdropping scenarios, employing Gaussian quadrature techniques.
- We validate our analytical findings through Monte Carlo simulations, which confirm their accuracy and demonstrate the superior performance of the proposed system. The results show that deploying FAS instead of TAS in the WPCN significantly enhances transmission reliability and security. Specifically, FAS-equipped NOMA users achieve substantially lower SOP and higher ASC compared to TAS-equipped users, under both external and internal eavesdropping scenarios.

Therefore, a key innovation of this work lies in leveraging the FAS to enhance physical-layer security in WPCNs. In contrast to TAS, FAS dynamically adapts the antenna port to optimize channel conditions, providing higher spatial diversity and improved signal quality. This flexibility significantly reduces SOP and increases ASC, thereby strengthening resilience against both external and internal eavesdropping. The proposed FAS-aided framework thus represents a substantial advancement over conventional TAS-based models in securing energy-harvesting NOMA communications.

1.3. Organization

The rest of this paper is organized as follows. Section 2 presents the system model, including the channel model and the NOMA-FAS scheme. Section 3 provides the secrecy performance analysis, where theoretical frameworks for SOP and ASC are derived. Section 4 discusses the numerical results that validate the analytical findings and finally, Section 5 concludes the paper.

1.4. Notation

We use boldface upper and lower case letters for matrices and vectors, e.g. $\mathbf{X}$ and $\mathbf{x}$, respectively. Moreover, $(\cdot)^T$, $(\cdot)^{-1}$, $|\cdot|$, $\max\{\cdot\}$, and $\det(\cdot)$ stand for the transpose, inverse, magnitude, maximum, and determinant operators, respectively.

2. System model

This section presents the system model, where a single-antenna transmitter communicates confidential information to multiple FAS-equipped users under a NOMA scheme. The description includes key assumptions, such as channel conditions and FAS adaptability, which are critical for analyzing secrecy metrics in the following sections. Note that unlike traditional TAS-based WPCNs that typically use either energy or information links in isolation, our model employs a dual-link architecture. The system leverages WPT from a power beacon (PB) to energize the transmitter, followed by confidential data transmission to multiple users using NOMA. This dual-hop model enables secure, energy-efficient communication, while introducing unique vulnerabilities that are specifically addressed using FAS-equipped receivers and compact secrecy analysis.

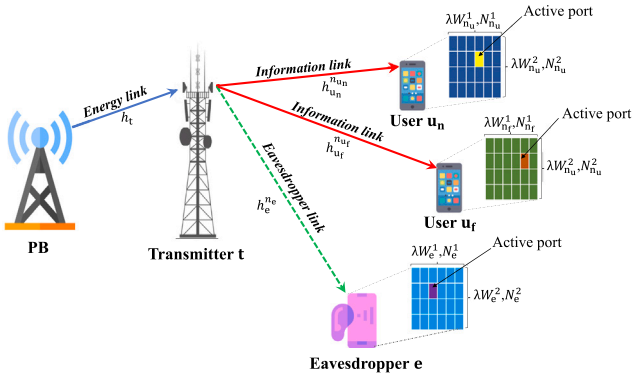

Fig. 1. System model: FAS-aided secure NOMA WPCN.

2.1. Channel model

We consider a PLS scenario in a WPCN, as illustrated in Fig. 1. In this setup, a transmitter t aims to deliver confidential information to two legitimate users, u_n and u_f, over wireless fading channels, while an external eavesdropper e attempts to intercept the transmitted signal. The transmitter broadcasts a superimposed signal containing the confidential message intended for the users under the NOMA scheme, utilizing energy wirelessly supplied by a PB. In this context, the wireless channel between the PB and the transmitter t is referred to as the *energy link*. The channels connecting the transmitter t to the near user u_n (referred to as the strong user) and the far user u_f (referred to as the weak user) are termed *information links*. Additionally, the channel between the transmitter t and the external eavesdropper e is designated as the *eavesdropper link*. Moreover, it is assumed that the far user u_f may act as an internal eavesdropper, attempting to decode the data signal intended for the near user u_n. It is assumed that both the PB and the transmitter t are single-antenna nodes, whereas the NOMA users $i \in u_n, u_f$ and the eavesdropper e are equipped with planar FASs. Specifically, the nodes $j \in \{u_n, u_f, e\}$ incorporate a grid structure comprising N_j^l ports, which are uniformly distributed along a linear space of length $W_j^l \lambda$ for $l \in \{1,2\}$. Consequently, the total number of ports is given by $N_j = N_j^1 \times N_j^2$, and the corresponding planar dimensions are $W_j = W_j^1 \lambda \times W_j^2 \lambda$. Additionally, to facilitate the transformation between the 2D and 1D index representations, a mapping function $\mathcal{F}\left(n_j\right) = \left(n_j^1, n_j^2\right)$ and its inverse $\mathcal{F}^{-1}\left(n_j^1, n_j^2\right) = n_j$ are defined, where $n_j \in \{1, \ldots, N_j\}$ and $n_j^l \in \left\{1, \ldots, N_j^l\right\}$.

The received signal at the n_jth port of the node j is expressed as

$$y_j^{n_j} = \sqrt{P_p \delta_j} h_{\mathrm{eq},j}^{n_j} \left(\sqrt{p_{u_n}} x_{u_n} + \sqrt{p_{u_f}} x_{u_f}\right) + z_j^{n_j}, \quad (1)$$

in which P_p represents the power transmitted by the PB, and $h_{\mathrm{eq},j}^{n_j} = h_t h_j^{n_j}$ denotes the equivalent channel coefficient at the n_jth port of node j. This coefficient encompasses the channel coefficients of the energy link h_t, the information links $h_i^{n_i}$, and the eavesdropper link $h_e^{n_e}$. Additionally, x_i represents the symbol transmitted to user i with unit power, while p_i specifies the power allocation factor for user i, such that $p_{u_1} + p_{u_2} = 1$. The term $z_j^{n_j}$ denotes the additive white Gaussian noise (AWGN) at the n_jth port of node j, characterized by zero mean and variance σ_j^2. Moreover, $\delta_j = L_p d_t^{-\alpha} d_j^{-\alpha}$ describes the path-loss, where L_p represents the frequency-dependent signal propagation loss, $\alpha > 2$ denotes the path-loss exponent, d_t is the distance between the PB and the transmitter t, and d_j is the distance between the transmitter t and node j.

Furthermore, the ports in the FAS can freely switch and are positioned in close proximity to each other, leading to spatial correlation in the channel coefficients at each NOMA FAS-equipped node. Assuming that the energy, information, and eavesdropper links experience

Rayleigh fading, the covariance between two arbitrary ports n_j and $\tilde{n}_j$ at each node j in a three-dimensional (3D) rich-scattering environment can be expressed as

$$\rho^{j}_{n_j,\tilde{n}_j} = \mathcal{J}_0\left(2\pi\sqrt{\left(\frac{n_j^1-\tilde{n}_j^1}{N_j^1-1}W_j^1\right)^2+\left(\frac{n_j^2-\tilde{n}_j^2}{N_j^2-1}W_j^2\right)^2}\right), \tag{2}$$

in which $\tilde{n}_j = \mathcal{F}^{-1}\left(\tilde{n}_j^1, \tilde{n}_j^2\right)$ so that $\tilde{n}_j^l \in \left\{1,\ldots,N_j^l\right\}$ and $\mathcal{J}_0(.)$ denotes the zero-order spherical Bessel function of the first kind.

Given the concept of FAS, we assume that only the optimal port, which maximizes the received signal-to-noise ratio (SNR) at node j, is activated. Additionally, we consider a scenario where the CSI is available to the external eavesdropper, enabling it to select the best port to maximize its SNR. This assumption represents a worst-case scenario, as the eavesdropper is provided with ideal operating conditions. Specifically, the external eavesdropper is assumed to perform perfect multi-user detection,[4] allowing it to differentiate between user data and completely eliminate inter-user interference. Moreover, due to the inherent spatial correlation among fluid antenna ports, acquiring full CSI requires only a limited number of port observations, irrespective of the total number of fluid antenna ports [40]. Consequently, the equivalent channel gain at node j is defined as

$$g_{\text{fas},j} = \max\left\{g_{\text{eq},1}^1,\ldots,g_{\text{eq},j}^{N_j}\right\} = g_{\text{eq},j}^{n_j^*}, \tag{3}$$

in which $g_{\text{eq},j}^{n_j^*} = \left|h_{\text{eq},j}^{n_j}\right|^2$ is the channel gain at n_jth port of node j and n_j^* denotes the best port index at node j that maximizes the channel gain, i.e.,

$$n_u^* = \arg\max_{n_u}\left\{\left|h_{\text{eq},j}^{n_j}\right|^2\right\}. \tag{4}$$

2.2. NOMA-FAS scheme

In accordance with the NOMA principle, the near FAS-equipped user u_n employs successive interference cancellation (SIC) as part of its optimal decoding strategy. This approach requires the far FAS-equipped user u_f to decode its signal directly while treating any interference as background noise. Assuming that only the optimal port, which maximizes the received signal-to-interference-plus-noise ratio (SINR) for the FAS-equipped users, is active, the SINR for the SIC process is formulated as

$$\gamma_{\text{sic}} = \frac{\overline{\gamma}_{\text{u}_\text{n}} p_{\text{u}_\text{f}} g_{\text{fas},\text{u}_\text{n}}}{\overline{\gamma}_{\text{u}_\text{n}} p_{\text{u}_\text{n}} g_{\text{fas},\text{u}_\text{n}} + 1}, \tag{5}$$

where $\overline{\gamma}_{\text{u}_\text{n}} = \frac{P_\text{p} L_\text{p}}{\sigma^2_{\text{u}_\text{n}} d_\text{t}^\alpha d_{\text{u}_\text{n}}^\alpha}$ denotes the average SNR for the near user u_n. After applying SIC, u_n eliminates the signal intended for u_f from its received signal and proceeds to decode its own required information. Consequently, the received SNR at the FAS-equipped user u_n is expressed as

$$\gamma_{\text{u}_\text{n}} = \overline{\gamma}_{\text{u}_\text{n}} p_{\text{u}_\text{n}} g_{\text{fas},\text{u}_\text{n}}. \tag{6}$$

Meanwhile, the far user u_f decodes its own signal directly but is unable to distinguish or cancel out the signal from the near user u_n within the superimposed transmission. Consequently, the SINR experienced by the far FAS-equipped user u_f is represented as

$$\gamma_{\text{u}_\text{f}} = \frac{\overline{\gamma}_{\text{u}_\text{f}} p_{\text{u}_\text{f}} g_{\text{fas},\text{u}_\text{f}}}{\overline{\gamma}_{\text{u}_\text{f}} p_{\text{u}_\text{n}} g_{\text{fas},\text{u}_\text{f}} + 1}, \tag{7}$$

where $\overline{\gamma}_{\text{u}_\text{f}} = \frac{P_\text{p} L_\text{p}}{\sigma^2_{\text{u}_\text{f}} d_\text{t}^\alpha d_{\text{u}_\text{f}}^\alpha}$ defines the average SNR for the near user.

[4] The assumption of perfect multi-user detection at the eavesdropper models a worst-case scenario. It enables conservative evaluation of secrecy performance and ensures the proposed scheme remains robust even under ideal eavesdropping conditions.

The external eavesdropper intercepts the transmitted signals from the transmitter. As a result, the SNR at the external eavesdropper e for decoding x_i is given by

$$\gamma_{\text{e},i} = \overline{\gamma}_\text{e} p_i g_{\text{fas,e}}, \tag{8}$$

where $\overline{\gamma}_\text{e} = \frac{P_\text{p} L_\text{p}}{\sigma_\text{e}^2 d_\text{t}^\alpha d_\text{e}^\alpha}$ represents the average SNR of the external eavesdropper.

In the case of internal eavesdropping, the far user attempts to decode the message intended for the near user after receiving x_{u_f}. Hence, assuming that x_{u_f} is decoded without error at the far user, the SNR at the far user u_f for decoding x_{u_n} is expressed as

$$\gamma_{\text{u}_\text{f},n} = \overline{\gamma}_{\text{u}_\text{f}} p_{\text{u}_\text{n}} g_{\text{fas},\text{u}_\text{f}}. \tag{9}$$

3. Secrecy performance analysis

In this section, we first introduce the distribution of the equivalent channel for the FAS-equipped nodes. Additionally, we present a concise derivation of key secrecy performance metrics, e.g., SOP and ASC, based on the distributions of the equivalent channel gains of FAS-equipped users. Due to the complexity introduced by correlated fading and antenna selection, the Gaussian quadrature method is employed to obtain compact, tractable expressions. The analytical results, supported by Monte Carlo simulations, quantitatively demonstrate that the proposed FAS-aided system achieves significantly lower SOP and higher ASC compared to traditional TAS-based models under both external and internal eavesdropping scenarios.

3.1. SOP analysis

3.1.1. Statistical characteristics

To analytically assess key secrecy performance metrics in the considered FAS-aided secure WPCN, the first step is to derive the distribution of the equivalent fading channel coefficients at the FAS-equipped nodes. Specifically, this involves calculating the maximum of N_j correlated random variables (RVs), each of which is the product of two independent exponentially-distributed RVs (as shown in (3)). Since the energy, information, and eavesdropper links experience Rayleigh fading, the corresponding channel gains $g_\text{t} = |h_\text{t}|^2$ and $g_j^{n_j} = \left|h_j^{n_j}\right|^2$ follow an exponential distribution with unit mean. Consequently, the cumulative distribution function (CDF) of the equivalent channel gain $g_{\text{eq},j}^{n_j} = g_\text{t} g_j^{n_j}$ at node j is derived as

$$F_{g_{\text{eq},j}^{n_j}}(g) = \int_0^\infty f_{g_\text{t}}(g_\text{t}) F_{g_j^{n_j}}\left(\frac{g}{g_\text{t}}\right)\text{d}g_\text{t} \tag{10}$$

$$= 1 - \int_0^\infty \exp\left(-\left(g_\text{t}+\frac{g}{g_\text{t}}\right)\right)\text{d}g_\text{t} \tag{11}$$

$$\overset{(a)}{=} 1 - 2\sqrt{g}\mathcal{K}_1\left(2\sqrt{g}\right), \tag{12}$$

in which $f_{g_\text{t}}(\cdot)$ and $F_{g_i^{n_i}}(\cdot)$ are the marginal PDF and CDF of exponentially-distributed g_t and $g_j^{n_j}$. Additionally, (a) is derived by employing the integral expression given in [41, 3.471.9], where $\mathcal{K}_1(\cdot)$ denotes the first-order modified Bessel function of the second kind.

Next, by applying the definition, the CDF of $g_{\text{fas},j}$ can be mathematically formulated as follows

$$F_{g_{\text{fas},j}}(g) = \Pr\left(\max\left\{g_{\text{eq},j}^1,\ldots,g_{\text{eq},j}^{N_j}\right\} \le g\right) \tag{13}$$

$$= \Pr\left(g_{\text{eq},j}^1 \le r,\ldots,g_{\text{eq},j}^{N_j} \le g\right) \tag{14}$$

$$= F_{g_{\text{eq},j}^1,\ldots,g_{\text{eq},j}^{N_j}}(g,\ldots,g), \tag{15}$$

where (15) represents the definition of the multivariate distribution for N_j correlated RVs $g_{\text{eq},j}^{n_j}$, where $n_j \in \left\{1,\ldots,N_j\right\}$. To derive this distribution, we apply Sklar's theorem [42], which allows us to construct the multivariate distribution of N_j correlated arbitrary RVs, such as $g_{\text{fas},j}$,

by utilizing only the corresponding marginal distributions. Therefore, the CDF of $g_{\text{fas},j}$, denoted as $F_{g_{\text{fas},j}}(g)$, can be expressed as

$$F_{g_{\text{fas},j}}(g) = \boldsymbol{\Phi}_{\mathbf{R}_j}\left(\phi^{-1}\left(F_{g_{\text{eq},j}^1}(g)\right),\ldots,\phi^{-1}\left(F_{g_{\text{eq},j}^{N_j}}(g)\right);\vartheta_j\right), \tag{16}$$

where $\phi^{-1}\left(F_{g_{\text{eq},j}^{n_j}}(g)\right) = \sqrt{2}\text{erf}^{-1}\left(2F_{g_{\text{eq},j}^{n_j}}(g)-1\right)$ represents the quantile function of the standard normal distribution, and ϑ_j denotes the dependence parameter, specifically the Gaussian copula parameter.[5] The term $\boldsymbol{\Phi}_{\mathbf{R}_j}$ refers to the joint CDF of the multivariate normal distribution, which has a zero mean vector and a correlation matrix $\mathbf{R}_j$.

$$\mathbf{R}_j = \begin{bmatrix} \varrho_{1,1}^j & \varrho_{1,2}^j & \cdots & \varrho_{1,N_j}^j \\ \varrho_{2,1}^j & \varrho_{2,2}^j & \cdots & \varrho_{2,N_j}^j \\ \vdots & \vdots & \ddots & \vdots \\ \varrho_{N_j,1}^j & \varrho_{N_j,2}^j & \cdots & \varrho_{N_j,N_j}^j \end{bmatrix}. \tag{17}$$

Therefore, using Sklar's theorem, the multivariate distribution is constructed from the marginal distributions via the Gaussian copula. The quantile transformation $\phi^{-1}(\cdot)$ maps the exponential marginal CDFs into the standard normal domain. Consequently, the resulting joint CDF of $g_{\text{fas},j}$ captures spatial correlation through the covariance matrix $\mathbf{R}_j$, which is derived from the antenna port positions using (2).

By applying the chain rule to (16), the PDF of $g_{\text{fas},j}$ is expressed as

$$f_{g_{\text{fas},j}}(g) = \sum_{n_j=1}^{N_j} \frac{\partial \boldsymbol{\Phi}_{\mathbf{R}_j}\left(\boldsymbol{\phi}_{N_j}^{-1}\right)}{\partial \phi^{-1}\left(F_{g_{\text{eq},j}^{n_j}}(g)\right)} \frac{f_{g_{\text{eq},j}^{n_j}}(g)}{\varphi\left(\phi^{-1}\left(F_{g_{\text{eq},j}^{n_j}}(g)\right)\right)}, \tag{18}$$

where $\varphi(x) = \frac{1}{\sqrt{2\pi}}\text{e}^{-\frac{x^2}{2}}$ is the standard normal PDF and

$$\boldsymbol{\phi}_{N_j}^{-1} = \left[\phi^{-1}\left(F_{g_{\text{eq},j}^1}(g)\right),\ldots,\phi^{-1}\left(F_{g_{\text{eq},j}^{N_j}}(g)\right)\right]^T. \tag{19}$$

Moreover, $f_{g_{\text{eq},j}^{n_j}}(g)$ is the PDF of the equivalent channel gain $g_{\text{eq},j}^{n_j} = g_{\text{t}}g_j^{n_j}$ at the node j, which is derived as

$$f_{g_{\text{eq},j}^{n_j}}(g) = 2\mathcal{K}_0\left(2\sqrt{g}\right), \tag{20}$$

where $\mathcal{K}_0$ denotes the zero-order modified Bessel function of the second kind.

Therefore, by inserting (12) into (16) and replacing (20) into (18), the CDF and PDF of $g_{\text{fas},j}(g)$ are derived as shown in (21) and (22), respectively, where $\mathbf{z}_j$ is defined in (23) (see Eqs. (21)–(23), (26), (27) in Box I).

3.1.2. External eavesdropping

Here, we derive the analytical expressions of the SOP for both the near and far users under the scenario of external eavesdropping.

The SOP is defined as the likelihood that the instantaneous secrecy capacity $C_{\text{s},i}^{\text{ext}}$ in the external eavesdropping scenario falls below a specified target secrecy rate $R_{\text{s},i} \geq 0$, which can be expressed as

$$P_{\text{sop},i}^{\text{ext}} = \Pr\left(C_{\text{s},i}^{\text{ext}} \leq R_{\text{s},i}\right), \tag{24}$$

where $C_{\text{s},i}^{\text{ext}}$ is defined as the difference between the channel capacities of the legitimate users and the eavesdropper links, i.e.,

$$C_{\text{s},i}^{\text{ext}} = \max\left\{\log_2\left(1+\gamma_i\right) - \log_2\left(1+\gamma_{\text{e},i}\right), 0\right\}. \tag{25}$$

[5] The Gaussian copula effectively captures the spatial correlation between fluid antenna ports, particularly when the fluid antenna size is large. In this context, the dependence parameter of the Gaussian copula can be approximated by the covariance between two arbitrary ports, i.e., $\varrho^i \approx \vartheta_i$ [43].

Theorem 1. *The SOP expressions of the near user* u_n *and the far user* u_n *in the proposed FAS-aided secure WPCN under the external eavesdropping scenario are given by (26) and (27), respectively, where* $\nu_m = \frac{\overline{R}_\text{n}\left(\overline{\gamma}_\text{e}p_{\text{u}_\text{n}}\epsilon_m+1\right)-1}{\overline{\gamma}_{\text{u}_\text{n}}p_{\text{u}_\text{n}}}$, $\mu_m = \frac{\overline{R}_\text{f}\left(1+\overline{\gamma}_\text{e}p_{\text{u}_\text{f}}\epsilon_m\right)-1}{\overline{\gamma}_{\text{u}_\text{f}}\left(p_{\text{u}_\text{f}}-p_{\text{u}_\text{n}}\left[\overline{R}_\text{f}\left(1+\overline{\gamma}_\text{e}p_{\text{u}_\text{f}}\epsilon_m\right)-1\right]\right)}$, *and* $\mathbf{z}_\text{e} = \left[\phi^{-1}\left(F_{g_{\text{eq,e}}^1}(\epsilon_m)\right),\ldots,\phi^{-1}\left(F_{g_{\text{eq,e}}^{N_\text{e}}}(\epsilon_m)\right)\right]^T$.

Proof. By substituting (6) and (8) into (24), we have

$$P_{\text{sop},\text{u}_\text{n}}^{\text{ext}} = \Pr\left(\frac{1+\gamma_{\text{u}_\text{n}}}{1+\gamma_{\text{e},\text{u}_\text{n}}} \leq 2^{R_{\text{s},\text{u}_\text{n}}}\right) \tag{28}$$

$$= \Pr\left(\frac{1+\overline{\gamma}_{\text{u}_\text{n}}p_{\text{u}_\text{n}}g_{\text{fas},\text{u}_\text{n}}}{1+\overline{\gamma}_\text{e}p_{\text{u}_\text{n}}g_{\text{fas,e}}} \leq \overline{R}_\text{n}\right) \tag{29}$$

$$= \Pr\left(g_{\text{fas},\text{u}_\text{n}} \leq \frac{\overline{R}_\text{n}\left(\overline{\gamma}_\text{e}p_{\text{u}_\text{n}}g_{\text{fas,e}}+1\right)-1}{\overline{\gamma}_{\text{u}_\text{n}}p_{\text{u}_\text{n}}}\right) \tag{30}$$

$$= \int_0^\infty F_{g_{\text{fas},\text{u}_\text{n}}}\left(\frac{\overline{R}_\text{n}\left(\overline{\gamma}_\text{e}p_{\text{u}_\text{n}}g+1\right)-1}{\overline{\gamma}_{\text{u}_\text{n}}p_{\text{u}_\text{n}}}\right) f_{g_{\text{fas,e}}}(g)\text{d}g, \tag{31}$$

where $\overline{R}_\text{n} = 2^{R_{\text{s},\text{u}_\text{n}}}$. After substituting the corresponding CDF and PDF into (31), it becomes evident that solving the integral analytically is intractable. Therefore, we apply the Gauss–Laguerre quadrature method, as outlined in the following lemma, to derive the SOP.

Lemma 1. *The Gauss–Laguerre quadrature is defined as [44]*

$$\int_0^\infty \Lambda(x)\,\text{d}x \approx \sum_{m=0}^{M} \text{e}^{\epsilon_m}\omega_m\Lambda\left(\epsilon_m\right), \tag{32}$$

where M *is the number of sample points used,* ϵ_m *denotes the* m*th root of Laguerre polynomial* $L_M\left(\epsilon_m\right)$*, and* $\omega_m = \frac{\epsilon_m}{2(M+1)^2L_{M+1}^2(\epsilon_m)}$ *represents the corresponding weight.*

Now, by applying Lemma 1 to (31), the expression for (26) is obtained, thus completing the proof. Similarly, or the SOP of the far user, we have

$$P_{\text{sop},\text{u}_\text{f}}^{\text{ext}} = \Pr\left(\frac{1+\gamma_{\text{u}_\text{f}}}{1+\gamma_{\text{e},\text{u}_\text{f}}} \leq 2^{R_{\text{s},\text{u}_\text{f}}}\right) \tag{33}$$

$$= \Pr\left(\frac{1+\frac{\overline{\gamma}_{\text{u}_\text{f}}p_{\text{u}_\text{f}}g_{\text{fas},\text{u}_\text{f}}}{\overline{\gamma}_{\text{u}_\text{f}}p_{\text{u}_\text{n}}g_{\text{fas},\text{u}_\text{f}}+1}}{1+\overline{\gamma}_\text{e}p_{\text{u}_\text{f}}g_{\text{fas,e}}} \leq \overline{R}_\text{f}\right) \tag{34}$$

$$= \Pr\left(g_{\text{fas},\text{u}_\text{f}} \leq \frac{\overline{R}_\text{f}\left(1+\overline{\gamma}_\text{e}p_{\text{u}_\text{f}}g_{\text{fas,e}}\right)-1}{\overline{\gamma}_{\text{u}_\text{f}}\left(p_{\text{u}_\text{f}}-p_{\text{u}_\text{n}}\left[\overline{R}_\text{f}\left(1+\overline{\gamma}_\text{e}p_{\text{u}_\text{f}}g_{\text{fas,e}}\right)-1\right]\right)}\right) \tag{35}$$

$$= \int_0^\infty F_{g_{\text{fas},\text{u}_\text{f}}}\left(\frac{\overline{R}_\text{f}\left(1+\overline{\gamma}_\text{e}p_{\text{u}_\text{f}}g\right)-1}{\overline{\gamma}_{\text{u}_\text{f}}\left(p_{\text{u}_\text{f}}-p_{\text{u}_\text{n}}\left[\overline{R}_\text{f}\left(1+\overline{\gamma}_\text{e}p_{\text{u}_\text{f}}g\right)-1\right]\right)}\right) \times f_{g_{\text{fas,e}}}(g)\text{d}g, \tag{36}$$

where $\overline{R}_\text{f} = 2^{R_{\text{s},\text{u}_\text{f}}}$. After substituting the corresponding CDF and PDF into (36), and applying Lemma 1, the expression for (27) is derived, thus completing the proof. □

3.1.3. Internal eavesdropping

Given the definition of the internal eavesdropping scenario, where the far user acts as an eavesdropper, the corresponding secrecy capacity is defined as

$$C_{\text{s},\text{u}_\text{n}}^{\text{int}} = \max\left\{\log_2\left(1+\gamma_{\text{u}_\text{n}}\right) - \log_2\left(1+\gamma_{\text{u}_\text{f},n}\right), 0\right\}, \tag{37}$$

$$F_{g_{\mathrm{fas},j}}(g)=\boldsymbol{\Phi}_{\mathbf{R}_j}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{g}\mathcal{K}_1\left(2\sqrt{g}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{g}\mathcal{K}_1\left(2\sqrt{g}\right)\right);\vartheta_j\right) \tag{21}$$

$$f_{g_{\mathrm{fas},j}}(g)=\frac{2\sqrt{2\pi}\mathcal{K}_0\left(2\sqrt{g}\right)}{\exp\left(-\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{g}\mathcal{K}_1\left(2\sqrt{g}\right)\right)\right)^2/2\right)}\sum_{n_j=1}^{N_j}\left.\frac{\partial\boldsymbol{\Phi}_{\mathbf{R}_j}\left(\mathbf{z}_j\right)}{\partial z_{n_j}}\right|_{z_{n_j}=\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{g}\mathcal{K}_1\left(2\sqrt{g}\right)\right)}, \tag{22}$$

$$\mathbf{z}_j=\left[\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{g}\mathcal{K}_1\left(2\sqrt{g}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{g}\mathcal{K}_1\left(2\sqrt{g}\right)\right)\right]^T \tag{23}$$

$$\begin{aligned}P_{\mathrm{sop},\mathrm{u_n}}^{\mathrm{ext}}\approx&\sum_{m=0}^{M}\frac{2\sqrt{2\pi}\mathcal{K}_0\left(2\sqrt{\epsilon_m}\right)\mathrm{e}^{\epsilon_m}\omega_m}{\exp\left(-\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\epsilon_m}\mathcal{K}_1\left(2\sqrt{\epsilon_m}\right)\right)\right)^2/2\right)}\sum_{n_\mathrm{e}=1}^{N_\mathrm{e}}\left.\frac{\partial\boldsymbol{\Phi}_{\mathbf{R}_\mathrm{e}}\left(\mathbf{z}_\mathrm{e}\right)}{\partial z_{n_\mathrm{e}}}\right|_{z_{n_\mathrm{e}}=\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\epsilon_m}\mathcal{K}_1\left(2\sqrt{\epsilon_m}\right)\right)}\\&\times\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_n}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\nu_m}\mathcal{K}_1\left(2\sqrt{\nu_m}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\nu_m}\mathcal{K}_1\left(2\sqrt{\nu_m}\right)\right);\vartheta_{\mathrm{u_n}}\right)\end{aligned} \tag{26}$$

$$\begin{aligned}P_{\mathrm{sop},\mathrm{u_n}}^{\mathrm{ext}}\approx&\sum_{m=0}^{M}\frac{2\sqrt{2\pi}\mathcal{K}_0\left(2\sqrt{\epsilon_m}\right)\mathrm{e}^{\epsilon_m}\omega_m}{\exp\left(-\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\epsilon_m}\mathcal{K}_1\left(2\sqrt{\epsilon_m}\right)\right)\right)^2/2\right)}\sum_{n_\mathrm{e}=1}^{N_\mathrm{e}}\left.\frac{\partial\boldsymbol{\Phi}_{\mathbf{R}_\mathrm{e}}\left(\mathbf{z}_\mathrm{e}\right)}{\partial z_{n_\mathrm{e}}}\right|_{z_{n_\mathrm{e}}=\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\epsilon_m}\mathcal{K}_1\left(2\sqrt{\epsilon_m}\right)\right)}\\&\times\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_f}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\mu_m}\mathcal{K}_1\left(2\sqrt{\mu_m}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\mu_m}\mathcal{K}_1\left(2\sqrt{\mu_m}\right)\right);\vartheta_{\mathrm{u_f}}\right)\end{aligned} \tag{27}$$

Box I.

$$\begin{aligned}P_{\mathrm{sop},\mathrm{u_n}}^{\mathrm{ext}}\approx&\sum_{m=0}^{M}\frac{2\sqrt{2\pi}\mathcal{K}_0\left(2\sqrt{\epsilon_m}\right)\mathrm{e}^{\epsilon_m}\omega_m}{\exp\left(-\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\epsilon_m}\mathcal{K}_1\left(2\sqrt{\epsilon_m}\right)\right)\right)^2/2\right)}\sum_{n_{\mathrm{u_f}}=1}^{N_{\mathrm{u_f}}}\left.\frac{\partial\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_f}}}\left(\mathbf{z}_{\mathrm{u_f}}\right)}{\partial z_{n_{\mathrm{u_f}}}}\right|_{z_{n_{\mathrm{u_f}}}=\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\epsilon_m}\mathcal{K}_1\left(2\sqrt{\epsilon_m}\right)\right)}\\&\times\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_n}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\zeta_m}\mathcal{K}_1\left(2\sqrt{\zeta_m}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\zeta_m}\mathcal{K}_1\left(2\sqrt{\zeta_m}\right)\right);\vartheta_{\mathrm{u_n}}\right)\end{aligned} \tag{39}$$

Box II.

and the corresponding SOP is defined as

$$P_{\mathrm{sop},\mathrm{u_n}}^{\mathrm{int}}=\Pr\left(C_{\mathrm{s},\mathrm{u_n}}^{\mathrm{int}}\le R_{\mathrm{s},\mathrm{u_n}}\right). \tag{38}$$

Theorem 2. *The SOP expression of the near user* $\mathrm{u_n}$ *in the proposed FAS-aided secure WPCN under the internal eavesdropping scenario is given by* (39) *in Box* II, *where* $\zeta_m=\frac{\overline{R}_\mathrm{n}\left(\overline{\gamma}_{\mathrm{u_f}}p_{\mathrm{u_n}}\epsilon_m+1\right)-1}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}$ *and* $\mathbf{z}_{\mathrm{u_f}}=\left[\phi^{-1}\left(F^{-1}_{g_{\mathrm{eq},\mathrm{u_f}}}(\epsilon_m)\right),\ldots,\phi^{-1}\left(F^{N_{\mathrm{u_f}}}_{g_{\mathrm{eq},\mathrm{u_f}}}(\epsilon_m)\right)\right]^T$.

Proof. As given by (38), we have

$$P_{\mathrm{sop},\mathrm{u_n}}^{\mathrm{int}}=\Pr\left(\frac{1+\gamma_{\mathrm{u_n}}}{1+\gamma_{\mathrm{u_f},n}}\le 2^{R_{\mathrm{s},\mathrm{u_n}}}\right) \tag{40}$$

$$=\Pr\left(\frac{1+\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}g_{\mathrm{fas},\mathrm{u_n}}}{1+\overline{\gamma}_{\mathrm{u_f}}p_{\mathrm{u_n}}g_{\mathrm{fas},\mathrm{u_f}}}\le\overline{R}_\mathrm{n}\right) \tag{41}$$

$$=\Pr\left(g_{\mathrm{fas},\mathrm{u_n}}\le\frac{\overline{R}_\mathrm{n}\left(\overline{\gamma}_{\mathrm{u_f}}p_{\mathrm{u_n}}g_{\mathrm{fas},\mathrm{u_f}}+1\right)-1}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}\right) \tag{42}$$

$$=\int_0^\infty F_{g_{\mathrm{fas},\mathrm{u_n}}}\left(\frac{\overline{R}_\mathrm{n}\left(\overline{\gamma}_{\mathrm{u_f}}p_{\mathrm{u_n}}g+1\right)-1}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}\right)f_{g_{\mathrm{fas},\mathrm{u_f}}}(g)\mathrm{d}g. \tag{43}$$

Now, by applying Lemma 1 to (43), (39) is derived and the proof is completed. □

3.2. ASC analysis

3.2.1. External eavesdropping

Given the definition of secrecy capacity in (25), the ASC under the external eavesdropping scenario is defined as

$$\overline{C}_{\mathrm{s},i}^{\mathrm{ext}}=\int_0^\infty\int_0^{\gamma_{\mathrm{u_n}}}C_{\mathrm{s},i}^{\mathrm{ext}}\left(\gamma_i,\gamma_{\mathrm{e},i}\right)f_{\gamma_i}\left(\gamma_i\right)f_{\gamma_{\mathrm{e},i}}\left(\gamma_{\mathrm{e},i}\right)\mathrm{d}\gamma_i\mathrm{d}\gamma_{\mathrm{e},i}, \tag{44}$$

where $f_{\gamma_i}\left(\gamma_i\right)$ and $f_{\gamma_{\mathrm{e},i}}\left(\gamma_{\mathrm{e},i}\right)$ are the PDFs of γ_i and $\gamma_{\mathrm{e},i}$, respectively, which can be obtained through the transformation of RVs.

Theorem 3. *The ASC expressions of the near user* $\mathrm{u_n}$ *and the far user* $\mathrm{u_n}$ *in the proposed FAS-aided secure WPCN under the external eavesdropping scenario are given by* (45) *and* (46), *respectively, where* $\eta_m=\frac{\epsilon_m}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}$, $\tau_m=\frac{\epsilon_m}{\overline{\gamma}_\mathrm{e}p_{\mathrm{u_f}}}$, $\xi_{\tilde{m}}=\frac{\psi_{\tilde{m}}}{\overline{\gamma}_{\mathrm{u_f}}\left(p_{\mathrm{u_f}}-\psi_{\tilde{m}}p_{\mathrm{u_n}}\right)}$, *and* $\chi_{\tilde{m}}=\frac{\psi_{\tilde{m}}}{\overline{\gamma}_\mathrm{e}p_{\mathrm{u_f}}}$ *(see Eqs.* (45), (46) *and* (56) *in Box* III*).*

Proof. By extending (44), we have [34]

$$\overline{C}_{\mathrm{s},i}^{\mathrm{ext}}=\frac{1}{\ln 2}\int_0^\infty\frac{\overline{F}_{\gamma_i}\left(\gamma_i\right)}{1+\gamma_i}F_{\gamma_{\mathrm{e},i}}\left(\gamma_i\right)\mathrm{d}\gamma_i, \tag{47}$$

where $\overline{F}_{\gamma_i}\left(\gamma_i\right)=1-F_{\gamma_i}\left(\gamma_i\right)$ represents the complementary CDF (CCDF) of $\gamma_{\mathrm{u_n}}$ and $F_{\gamma_{\mathrm{e},i}}\left(\gamma_i\right)$ is the CDF of $\gamma_{\mathrm{e},i}$. By applying the RV transformation technique to (21), the CDF expressions of the node j are given by

$$F_{\gamma_{\mathrm{u_n}}}(\gamma)=F_{g_{\mathrm{fas},\mathrm{u_n}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}\right), \tag{48}$$

$$\overline{C}_{\mathrm{s,u_n}}^{\mathrm{ext}} \approx \frac{1}{\ln 2}\sum_{m=0}^{M}\frac{\mathrm{e}^{\epsilon_m}\omega_m}{1+\epsilon_m}\left[1-\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_n}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\eta_m}\mathcal{K}_1\left(2\sqrt{\eta_m}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\eta_m}\mathcal{K}_1\left(2\sqrt{\eta_m}\right)\right);\vartheta_{\mathrm{u_n}}\right)\right]$$
$$\times\,\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{e}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\tau_m}\mathcal{K}_1\left(2\sqrt{\tau_m}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\tau_m}\mathcal{K}_1\left(2\sqrt{\tau_m}\right)\right);\vartheta_{\mathrm{e}}\right) \tag{45}$$

$$\overline{C}_{\mathrm{s,u_f}}^{\mathrm{ext}} \approx \frac{p_{\mathrm{u_f}}}{p_{\mathrm{u_n}}2\ln 2}\sum_{\tilde{m}=0}^{\tilde{M}}\frac{\mathrm{e}^{\psi_m}\tilde{\omega}_{\tilde{m}}}{1+\psi_{\tilde{m}}}\left[1-\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_f}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\xi_{\tilde{m}}}\mathcal{K}_1\left(2\sqrt{\xi_{\tilde{m}}}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\xi_{\tilde{m}}}\mathcal{K}_1\left(2\sqrt{\xi_{\tilde{m}}}\right)\right);\vartheta_{\mathrm{u_f}}\right)\right]$$
$$\times\,\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{e}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\chi_{\tilde{m}}}\mathcal{K}_1\left(2\sqrt{\chi_{\tilde{m}}}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\chi_{\tilde{m}}}\mathcal{K}_1\left(2\sqrt{\chi_{\tilde{m}}}\right)\right);\vartheta_{\mathrm{e}}\right) \tag{46}$$

$$\overline{C}_{\mathrm{s,u_n}}^{\mathrm{int}} \approx \frac{1}{\ln 2}\sum_{m=0}^{M}\frac{\mathrm{e}^{\epsilon_m}\omega_m}{1+\epsilon_m}\left[1-\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_n}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\eta_m}\mathcal{K}_1\left(2\sqrt{\eta_m}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\eta_m}\mathcal{K}_1\left(2\sqrt{\eta_m}\right)\right);\vartheta_{\mathrm{u_n}}\right)\right]$$
$$\times\,\boldsymbol{\Phi}_{\mathbf{R}_{\mathrm{u_f}}}\left(\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\upsilon_m}\mathcal{K}_1\left(2\sqrt{\upsilon_m}\right)\right),\ldots,\sqrt{2}\mathrm{erf}^{-1}\left(1-4\sqrt{\upsilon_m}\mathcal{K}_1\left(2\sqrt{\upsilon_m}\right)\right);\vartheta_{\mathrm{u_f}}\right) \tag{56}$$

Box III.

$$F_{\gamma_{\mathrm{u_f}}}(\gamma)=\begin{cases}F_{g_{\mathrm{fas,u_f}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{u_f}}\left(p_{\mathrm{u_f}}-\gamma p_{\mathrm{u_n}}\right)}\right), & 0\le\gamma<\frac{p_{\mathrm{u_f}}}{p_{\mathrm{u_n}}},\\ 1, & \gamma\ge\frac{p_{\mathrm{u_f}}}{p_{\mathrm{u_n}}},\end{cases} \tag{49}$$

$$F_{\gamma_{\mathrm{e,u_n}}}(\gamma)=F_{g_{\mathrm{fas,e}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{e}}p_{\mathrm{u_n}}}\right), \tag{50}$$

and

$$F_{\gamma_{\mathrm{e,u_f}}}(\gamma)=F_{g_{\mathrm{fas,e}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{e}}p_{\mathrm{u_f}}}\right). \tag{51}$$

After inserting (48) and (49) into (47), $\overline{C}_{\mathrm{s},i}^{\mathrm{ext}}$ can be rewritten as

$$\overline{C}_{\mathrm{s,u_n}}^{\mathrm{ext}}=\frac{1}{\ln 2}\int_0^{\infty}\frac{1-F_{g_{\mathrm{fas,u_n}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}\right)}{1+\gamma}F_{g_{\mathrm{fas,e}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{e}}p_{\mathrm{u_n}}}\right)\mathrm{d}\gamma, \tag{52}$$

and

$$\overline{C}_{\mathrm{s,u_f}}^{\mathrm{ext}}=\frac{1}{\ln 2}\int_0^{\frac{p_{\mathrm{uf}}}{p_{\mathrm{u_n}}}}\frac{1-F_{g_{\mathrm{fas,u_f}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{u_f}}\left(p_{\mathrm{u_f}}-\gamma p_{\mathrm{u_n}}\right)}\right)}{1+\gamma}\times F_{g_{\mathrm{fas,e}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{e}}p_{\mathrm{u_n}}}\right)\mathrm{d}\gamma. \tag{53}$$

It is clear that solving (52) and (53) directly is mathematically complex. Therefore, by applying Lemma 1 to (52), $\overline{C}_{\mathrm{s,u_n}}^{\mathrm{ext}}$ is obtained as (45), completing the proof. For $\overline{C}_{\mathrm{s,u_f}}^{\mathrm{ext}}$, we utilize the Gauss–Legendre quadrature method, which is defined by the following lemma.

Lemma 2. *The Gauss–Legendre quadrature is defined as [44]*

$$\int_a^b\Lambda(x)\approx\frac{b-a}{2}\sum_{\tilde{m}}^{\tilde{M}}\tilde{\omega}_{\tilde{m}}\Lambda\left(\frac{b-a}{2}\psi_{\tilde{m}}+\frac{b+a}{2}\right), \tag{54}$$

where $\tilde{M}$ is the number of sample points used, $\psi_{\tilde{m}}$ is the $\tilde{m}$th root of Legendre polynomial $P_{\tilde{m}}(\psi_{\tilde{m}})$, and $\tilde{\omega}_{\tilde{m}}=\frac{2}{\left(1-\psi_{\tilde{m}}^2\right)\left[P'_{\tilde{m}}(\psi_{\mathrm{m}})\right]^2}$ denotes the corresponding quadrature weight.

Now, by applying Lemma 2, (46) is derived and the proof is accomplished. □

3.2.2. Internal eavesdropping

Based on the secrecy capacity definition in (37), the ASC under the internal eavesdropping scenario is given by

$$\overline{C}_{\mathrm{s},i}^{\mathrm{int}}=\int_0^{\infty}\int_0^{\gamma_{\mathrm{u_n}}}C_{\mathrm{s},i}^{\mathrm{ext}}\left(\gamma_i,\gamma_{\mathrm{e},i}\right)f_{\gamma_i}\left(\gamma_i\right)f_{\gamma_{\mathrm{e},i}}\left(\gamma_{\mathrm{e},i}\right)\mathrm{d}\gamma_i\mathrm{d}\gamma_{\mathrm{e},i}. \tag{55}$$

Theorem 4. *The ASC expression of the near user $\mathrm{u_n}$ and the far user $\mathrm{u_n}$ in the proposed FAS-aided secure WPCN under the internal eavesdropping scenario is given by (56), where $\eta_m=\frac{\epsilon_m}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}$ and $\upsilon_m=\frac{\epsilon_m}{\overline{\gamma}_{\mathrm{u_f}}p_{\mathrm{u_n}}}$.*

Proof. By extending (55), we have

$$\overline{C}_{\mathrm{s,u_n}}^{\mathrm{int}}=\frac{1}{\ln 2}\int_0^{\infty}\frac{\overline{F}_{\gamma_{\mathrm{u_n}}}\left(\gamma_{\mathrm{u_n}}\right)}{1+\gamma_{\mathrm{u_n}}}F_{\gamma_{\mathrm{u_f},n}}\left(\gamma_{\mathrm{u_n}}\right)\mathrm{d}\gamma_{\mathrm{u_n}}, \tag{57}$$

where $F_{\gamma_{\mathrm{u_f},n}}\left(\gamma_{\mathrm{u_n}}\right)$ denotes the CDF of $\gamma_{\mathrm{u_f},n}$, which is derived using the RV transformation technique to (9), i.e.,

$$F_{\gamma_{\mathrm{u_f},n}}(\gamma)=F_{g_{\mathrm{fas,u_f}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{u_f}}p_{\mathrm{u_n}}}\right). \tag{58}$$

Now, by substituting (58) and (48) in (57), we have

$$\overline{C}_{\mathrm{s,u_n}}^{\mathrm{int}}=\frac{1}{\ln 2}\int_0^{\infty}\frac{1-F_{g_{\mathrm{fas,u_n}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{u_n}}p_{\mathrm{u_n}}}\right)}{1+\gamma}F_{g_{\mathrm{fas,u_f}}}\left(\frac{\gamma}{\overline{\gamma}_{\mathrm{u_f}}p_{\mathrm{u_n}}}\right)\mathrm{d}\gamma. \tag{59}$$

After substituting the corresponding CDFs into (59) and applying Lemma 1, (56) is obtained, completing the proof. □

4. Numerical results

In this section, we evaluate the analytical derivations of the SOP and ASC, validating them through a thorough comparison with Monte Carlo simulations. For this evaluation, we define the channel model parameters as $p_{\mathrm{u_n}}=0.4$, $p_{\mathrm{u_f}}=0.6$, $\alpha=3$, $L_{\mathrm{p}}=1$, $d_{\mathrm{t}}=100$ m, $=d_{\mathrm{u_n}}=20$ m, $d_{\mathrm{u_f}}=60$ m, $d_{\mathrm{e}}=100$ m, $\sigma_i^2=-90$ dBm, $\sigma_{\mathrm{e}}^2=-80$ dBm $P_{\mathrm{p}}=30$ dBm, $R_{\mathrm{s},i}=0.5$ bps, $N_{\mathrm{e}}=4$, $W_{\mathrm{e}}=1\lambda^2$, $M=\tilde{M}=2$. The selected values of N_j and W_j follow guidelines in [25,27–29], ensuring sufficient spatial resolution while accounting for practical deployment size. We analyze performance for a range of values to assess scalability. Additionally, since the analytical derivations are expressed in terms of the joint multivariate normal distribution, we numerically implement these calculations using MATLAB, specifically the `copulacdf` and `copulapdf` functions. To further enhance the simulation, we apply the algorithm introduced in [43] to generate the Gaussian copula within the context of the system model under consideration.

Fig. 2 indicates the performance of SOP for NOMA user i in terms of the average SNR $\overline{\gamma}_i$ over the external eavesdropping scenario. First of all, it can be observed that the near user $\mathrm{u_n}$, for both FAS and TAS,

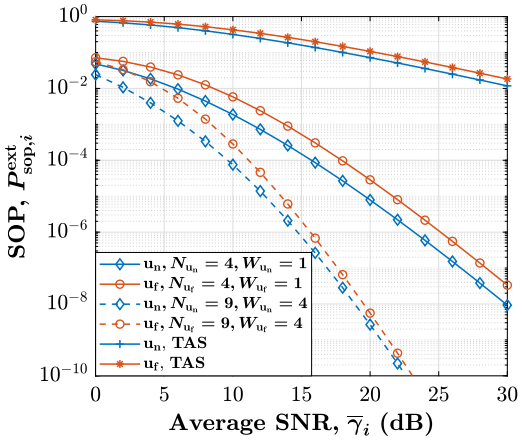

Fig. 2. The external SOP of user i versus the average SNR $\overline{\gamma}_i$ when $\overline{\gamma}_e = 0$ dB.

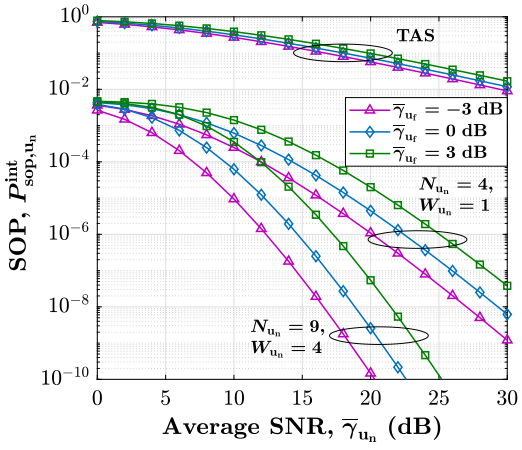

Fig. 3. The internal SOP of user $\mathrm{u_n}$ versus the average SNR $\overline{\gamma}_{\mathrm{u_n}}$ when $N_{\mathrm{u_f}} = 4$ and $W_{\mathrm{u_f}} = 1\lambda^2$.

achieves a lower SOP compared to the far user $\mathrm{u_f}$. The main reason for this is that, despite $\mathrm{u_n}$ having a lower power allocation, it benefits from the SIC process, which allows it to mitigate interference and decode its signal with higher reliability, leading to improved security and, consequently, a lower SOP. Additionally, we observe that when the NOMA user i benefits from the FAS, the SOP is significantly lower compared to when the user is equipped with the TAS. The advantage of FAS lies in its ability to dynamically adjust the antenna configuration, which improves signal quality and enhances system performance, thereby reducing the likelihood of secrecy outage. For instance, we observe that the SOP of the near FAS-equipped NOMA user $\mathrm{u_n}$ with $N_{\mathrm{u_n}} = 9$ and $W_{\mathrm{u_n}} = 4\lambda^2$ is on the order of 10^{-6} when $\overline{\gamma}_{\mathrm{u_n}} = 15$ dB, whereas the SOP for the same user under TAS is approximately 10^{-1}. It is also observed that the by simultaneously increasing N_i and W_i, spatial correlation between fluid antenna ports becomes balanced, and consequently lower SOP is obtained.

Fig. 3 illustrates the behavior of the SOP in terms of $\overline{\gamma}_{\mathrm{u_n}}$ when the far user $\mathrm{u_f}$ acts as an internal eavesdropper. We can see for a fixed value of $\overline{\gamma}_{\mathrm{u_f}}$, the SOP of the near user $u_{\mathrm{u_n}}$ decreases as $\overline{\gamma}_{\mathrm{u_n}}$ increases since the near NOMA user experience better channel condition than the internal eavesdropper (i.e., the far user). Furthermore, it can be observed that increasing $\overline{\gamma}_{\mathrm{u_f}}$ leads to a higher SOP, which is reasonable since the channel conditions of the internal eavesdropper improve. Additionally, by comparing Figs. 2 and 3, we can observe that the SOP of the near user $\mathrm{u_n}$ in the internal eavesdropping scenario performs better than in the external eavesdropping case. The main reason behind

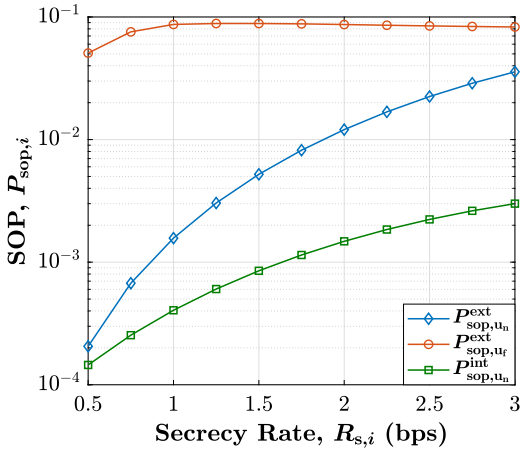

Fig. 4. The SOP of user i versus the secrecy rate $R_{\mathrm{s},i}$ when $N_j = 4$ and $W_j = 1\lambda^2$.

this is that in the internal eavesdropping scenario, the far user $\mathrm{u_f}$ (acting as the eavesdropper) typically experiences a weaker signal due to their distance from the transmitter, which makes it more difficult for them to decode the message. In contrast, an external eavesdropper, who may be located in a more favorable position with respect to the signal transmission, could intercept the signal more easily, leading to a higher likelihood of successful eavesdropping. Furthermore, power control strategies and PLS techniques can be more effectively optimized when the eavesdropper is internal, allowing the system to enhance the near user's security by minimizing the interference and signal leakage to the far user. Therefore, although the impact of external and internal eavesdroppers on the near user's SOP can vary significantly depending on specific factors, such as power control strategies and the effectiveness of PLS techniques, in most typical scenarios, the near user's SOP is lower (indicating more secure transmission) under internal eavesdropping compared to external eavesdropping.

Fig. 4 indicates the relationship between the SOP and secrecy rate $R_{\mathrm{s},i}$ for the FAS-equipped NOMA user i. It is observed that when $R_{\mathrm{s},i}$ is very low, it becomes easier for the secrecy capacity to exceed the target secrecy rate, resulting in low SOP for both the near user and the far user. Specifically, since the near user has a strong legitimate channel due to its proximity to the transmitter, ensuring a high achievable secrecy capacity, the SOP of $\mathrm{u_n}$ is very low in both the external and internal eavesdropping scenarios. The far user $\mathrm{u_f}$ has a weaker legitimate channel because of its distance from the transmitter, however, for small $R_{\mathrm{s},\mathrm{u_f}}$ even the far user's capacity can exceed the threshold, leading to a low SOP for $\mathrm{u_f}$. As the target secrecy rate increases, it becomes more difficult for the secrecy capacity to exceed $R_{\mathrm{s},i}$, causing the SOP to rise for both NOMA users. In this case, while $\mathrm{u_n}$ can still maintain a relatively low SOP due to its strong legitimate channel in both the external and internal eavesdropping scenarios, the SOP will steadily increase as $R_{\mathrm{s},\mathrm{u_n}}$ rises further. For the far user $\mathrm{u_f}$, the SOP rises much faster as $R_{\mathrm{s},\mathrm{u_f}}$ grows compared to the near user, because the far user's legitimate channel is weaker.

Figs. 5 and 6 illustrate the performance of the ASC in terms of the average SNR, $\overline{\gamma}_i$, under the external and internal eavesdropping scenarios, respectively. In both scenarios, we observe that as $\overline{\gamma}_i$ increases, the ASC of user i initially improves due to the dominant enhancement in the information link compared to the eavesdropper's link. However, the ASC eventually approaches a saturation point in the high-SNR regime, where further increases in transmit power fail to significantly boost the ASC. This is primarily because the relative difference between the information and eavesdropper channels stabilizes, and additional SNR gains benefit both channels similarly, limiting further improvements in secrecy capacity. Moreover, it is evident that FAS-equipped NOMA

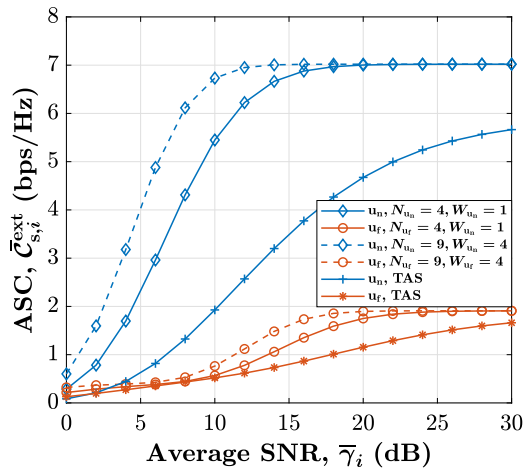

Fig. 5. The external ASC of user i versus the average SNR $\bar{\gamma}_i$.

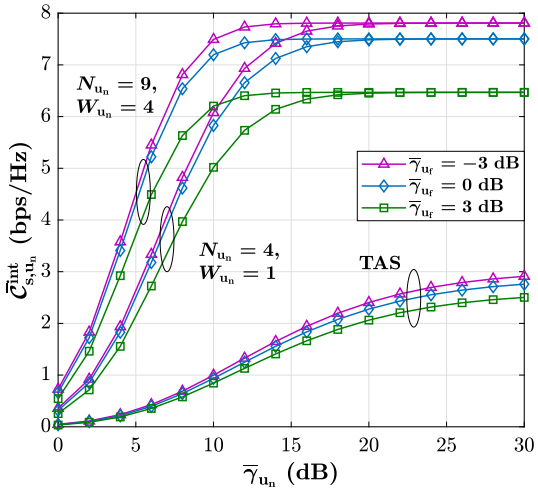

Fig. 6. The internal ASC of user u_n versus the average SNR $\bar{\gamma}_{u_n}$ when $N_{u_f} = 4$ and $W_{u_f} = 1\lambda^2$.

Table 1
Comparison of TAS vs. FAS secrecy performance.

Metric	TAS performance	FAS performance
SOP (far user)	1.07×10^{-1}	2.86×10^{-5}
SOP (near user)	7.21×10^{-2}	7.88×10^{-6}
ASC (far user)	1.15 bps/Hz	1.75 bps/Hz
ASC (near user)	4.67 bps/Hz	7.00 bps/Hz

users achieve higher ASC values compared to the TAS case in both external and internal eavesdropping scenarios. Additionally, we observe that increasing the number of fluid antenna ports over a larger fluid antenna size results in higher ASC values, as the spatial separation between ports becomes more balanced.

To further highlight the performance advantage of the proposed FAS-aided system, Table 1 presents a comparative summary of key secrecy metrics under a representative scenario with an average SNR of 20 dB, $N_j = 4$ antenna ports, and a FAS window size $W_j = 1\lambda^2$. As shown, the FAS-based design achieves significantly lower SOP and higher ASC than the TAS-based counterpart.

5. Conclusion

This study focused on evaluating the influence of FAS on the security performance of WPCNs. We proposed a framework where the transmitter relies on energy harvesting from a power beacon to transmit secure information to FAS-enabled users while countering the threats posed by both external and internal eavesdroppers. The use of NOMA added complexity by introducing a dual role for the far user, which could also act as an internal eavesdropper. To address these challenges, we conducted a thorough analysis of the equivalent channel characteristics at each node. Based on these derivations, we developed concise expressions for critical security metrics, such as the SOP and the ASC, using the Gaussian quadrature technique. The results of this research highlight the potential of FAS to enhance security in energy-constrained wireless systems and provide a theoretical foundation for designing robust communication protocols under such scenarios. Future work may explore the integration of FAS into more complex WPCN architectures, such as those involving cooperative relaying, full-duplex energy harvesting, or distributed antenna systems, to further enhance secure and energy-efficient communication. Additionally, real-world implementation of FAS involves challenges such as hardware cost, antenna control precision, and integration with mobile platforms. These practical aspects will be investigated through experimental prototypes and adaptive control mechanisms.

CRediT authorship contribution statement

Farshad Rostami Ghadi: Writing – original draft, Software, Conceptualization, Visualization, Investigation, Validation, Methodology, Data curation. **Masoud Kaveh:** Visualization, Methodology, Writing – original draft, Software, Data curation, Validation, Investigation, Conceptualization. **Kai-Kit Wong:** Writing – review & editing, Resources, Supervision, Funding acquisition, Validation, Project administration, Formal analysis. **Diego Martín:** Writing – review & editing, Software, Funding acquisition, Data curation, Validation, Resources, Formal analysis. **Riku Jäntti:** Visualization, Supervision, Project administration, Writing – review & editing, Resources, Funding acquisition, Formal analysis. **Zheng Yan:** Validation, Project administration, Writing – review & editing, Resources, Formal analysis, Supervision, Funding acquisition.

Declaration of competing interest

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

Data availability

No data was used for the research described in the article.

References

[1] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, M.F. Imani, Y.C. Eldar, Near-field wireless power transfer for 6G internet of everything mobile networks: Opportunities and challenges, IEEE Commun. Mag. 60 (3) (2022) 12–18.
[2] G. Moloudian, M. Hosseinifard, S. Kumar, R.B. Simorangkir, J.L. Buckley, C. Song, G. Fantoni, B. O'Flynn, RF energy harvesting techniques for battery-less wireless sensing, industry 4.0 and internet of things: A review, IEEE Sensors J. 24 (5) (2024) 5732–5745.
[3] S. Bi, Y. Zeng, R. Zhang, Wireless powered communication networks: An overview, IEEE Wirel. Commun. 23 (2) (2016) 10–18.
[4] X. Wang, J. Li, Z. Ning, Q. Song, L. Guo, S. Guo, M.S. Obaidat, Wireless powered mobile edge computing networks: A survey, ACM Comput. Surv. 55 (13s) (2023) 1–37.
[5] L. Huang, R. Nan, K. Chi, Q. Hua, K. Yu, N. Kumar, M. Guizani, Throughput guarantees for multi-cell wireless powered communication networks with non-orthogonal multiple access, IEEE Trans. Veh. Technol. 71 (11) (2022) 12104–12116.
[6] A. Mahmood, A. Ahmed, M. Naeem, M.R. Amirzada, A. Al-Dweik, Weighted utility aware computational overhead minimization of wireless power mobile edge cloud, Comput. Commun. 190 (2022) 178–189.

[7] J. Chen, L. Zhang, Y.-C. Liang, X. Kang, R. Zhang, Resource allocation for wireless-powered IoT networks with short packet communication, IEEE Trans. Wirel. Commun. 18 (2) (2019) 1447–1461.
[8] T.-H. Vu, S. Kim, Performance evaluation of power-beacon-assisted wireless-powered NOMA IoT-based systems, IEEE Internet Things J. 8 (14) (2021) 11655–11665.
[9] D.-T. Do, M.-S. Van Nguyen, T.N. Nguyen, X. Li, K. Choi, Enabling multiple power beacons for uplink of NOMA-enabled mobile edge computing in wirelessly powered IoT, IEEE Access 8 (2020) 148892–148905.
[10] K. Han, K. Huang, Wirelessly powered backscatter communication networks: Modeling, coverage, and capacity, IEEE Trans. Wirel. Commun. 16 (4) (2017) 2548–2561.
[11] F.R. Ghadi, F.J. Martin-Vega, F.J. López-Martínez, Capacity of backscatter communication under arbitrary fading dependence, IEEE Trans. Veh. Technol. 71 (5) (2022) 5593–5598.
[12] B. Lyu, Z. Yang, G. Gui, Y. Feng, Wireless powered communication networks assisted by backscatter communication, IEEE Access 5 (2017) 7254–7262.
[13] M. Kaveh, F. Rostami Ghadi, R. Jäntti, Z. Yan, Secrecy performance analysis of backscatter communications with side information, Sensors 23 (20) (2023) 8358.
[14] G.K. Ijemaru, K.L.M. Ang, J.K. Seng, Wireless power transfer and energy harvesting in distributed sensor networks: Survey, opportunities, and challenges, Int. J. Distrib. Sens. Netw. 18 (3) (2022) 15501477211067740.
[15] W. Liu, K.T. Chau, X. Tian, H. Wang, Z. Hua, Smart wireless power transfer—opportunities and challenges, Renew. Sustain. Energy Rev. 180 (2023) 113298.
[16] M. Kaveh, Z. Yan, R. Jantti, Secrecy performance analysis of RIS-aided smart grid communications, IEEE Trans. Ind. Inform. 20 (4) (2024) 5415–5427.
[17] A. Shafiqurrahman, V. Khadkikar, A.K. Rathore, Vehicle-to-vehicle (V2V) power transfer: Electrical and communication developments, IEEE Trans. Transp. Electrification 10 (3) (2024) 6258–6284.
[18] M. Li, Y. Zhang, K. Li, Y. Zhang, K. Xu, X. Liu, S. Zhong, J. Cao, Self-powered wireless sensor system for water monitoring based on low-frequency electromagnetic-pendulum energy harvester, Energy 251 (2022) 123883.
[19] S. Wang, X. Fu, R. Ruby, Z. Li, Pilot spoofing detection for massive MIMO mmwave communication systems with a cooperative relay, Comput. Commun. 202 (2023) 33–41.
[20] K.K. Wong, A. Shojaeifard, K.F. Tong, Y. Zhang, Fluid antenna systems, IEEE Trans. Wirel. Commun. 20 (3) (2021) 1950–1962.
[21] K.K. Wong, A. Shojaeifard, K.F. Tong, Y. Zhang, Performance limits of fluid antenna systems, IEEE Commun. Lett. 24 (11) (2020) 2469–2472.
[22] C. Wang, Z. Li, K.K. Wong, R. Murch, C.B. Chae, S. Jin, AI-empowered fluid antenna systems: Opportunities, challenges, and future directions, IEEE Wirel. Commun. 31 (5) (2024) 34–41.
[23] W.K. New, K.K. Wong, H. Xu, C. Wang, F.R. Ghadi, J. Zhang, J. Rao, R. Murch, P. Ramírez-Espinosa, D. Morales-Jimenez, C.B. Chae, A tutorial on fluid antenna system for 6G networks: Encompassing communication theory, optimization methods and hardware designs, IEEE Commun. Surv. Tutor. (2024).
[24] K.K. Wong, W.K. New, X. Hao, K.F. Tong, C.B. Chae, Fluid antenna system—part I: Preliminaries, IEEE Commun. Lett. 27 (8) (2023) 1919–1923.
[25] W.K. New, K.K. Wong, H. Xu, K.F. Tong, C.B. Chae, Fluid antenna system: New insights on outage probability and diversity gain, IEEE Trans. Wirel. Commun. 23 (1) (2023) 128–140.
[26] F. Rostami Ghadi, K.-K. Wong, W.K. New, H. Xu, R. Murch, Y. Zhang, On performance of RIS-aided fluid antenna systems, IEEE Wirel. Commun. Lett. 13 (8) (2024) 2175–2179.
[27] F.R. Ghadi, M. Kaveh, K.K. Wong, R. Jäntti, Z. Yan, On performance of FAS-aided wireless powered NOMA communication systems, in: Proc. 2024 20th Int. Conf. Wireless and Mobile Computing, Networking and Communications, WiMob, 2024, pp. 496–501.
[28] X. Lin, H. Yang, Y. Zhao, J. Hu, K.K. Wong, Performance analysis of integrated data and energy transfer assisted by fluid antenna systems, in: Proc. ICC 2024 - IEEE Int. Conf. Commun., 2024, pp. 2761–2766.
[29] F.R. Ghadi, M. Kaveh, K.K. Wong, Performance analysis of FAS-aided backscatter communications, IEEE Wirel. Commun. Lett. 13 (9) (2024) 2412–2416.
[30] Y. Ye, L. You, J. Wang, H. Xu, K.K. Wong, X. Gao, Fluid antenna-assisted MIMO transmission exploiting statistical CSI, IEEE Commun. Lett. 28 (1) (2024) 223–227.
[31] X. Jiang, C. Zhong, X. Chen, T.Q. Duong, T.A. Tsiftsis, Z. Zhang, Secrecy performance of wirelessly powered wiretap channels, IEEE Trans. Commun. 64 (9) (2016) 3858–3871.
[32] Y. Huang, P. Zhang, Q. Wu, J. Wang, Secrecy performance of wireless powered communication networks with multiple eavesdroppers and outdated CSI, IEEE Access 6 (2018) 33774–33788.
[33] K. Cao, H. Ding, L. Lv, Z. Su, J. Tao, F. Gong, B. Wang, Physical-layer security for intelligent-reflecting-surface-aided wireless-powered communication systems, IEEE Internet Things J. 10 (20) (2023) 18097–18110.
[34] F.R. Ghadi, K.K. Wong, F.J. López-Martínez, W.K. New, H. Xu, C.B. Chae, Physical layer security over fluid antenna systems: Secrecy performance analysis, IEEE Trans. Wirel. Commun. 23 (12) (2024) 18201–18213.
[35] J.D. Vega-Sánchez, L. Urquiza-Aguiar, H.R.C. Mora, N.V.O. Garzón, D.P.M. Osorio, Fluid antenna system: Secrecy outage probability analysis, IEEE Trans. Veh. Technol. 73 (8) (2024) 11458–11469.
[36] F.R. Ghadi, K.-K. Wong, M. Kaveh, F.J. Lopez-Martinez, W.K. New, H. Xu, Secrecy performance analysis of RIS-aided fluid antenna systems, in: 2025 IEEE Wireless Communications and Networking Conference, WCNC, Milan, Italy, 2025.
[37] W.K. New, K.K. Wong, H. Xu, K.F. Tong, C.B. Chae, Y. Zhang, Fluid antenna system enhancing orthogonal and non-orthogonal multiple access, IEEE Commun. Lett. (2023).
[38] L. Tlebaldiyeva, S. Arzykulov, T.A. Tsiftsis, G. Nauryzbayev, Full-duplex cooperative NOMA-based mmwave networks with fluid antenna system (FAS) receivers, in: Proc. 2023 Int. Balkan Conf. Commun. Networking, BalkanCom, 2023, pp. 1–6.
[39] J. Zheng, T. Wu, X. Lai, C. Pan, M. Elkashlan, K.K. Wong, FAS-assisted NOMA short-packet communication systems, IEEE Trans. Veh. Technol. (2024).
[40] N. Waqar, K.K. Wong, K.F. Tong, A. Sharples, Y. Zhang, Deep learning enabled slow fluid antenna multiple access, IEEE Commun. Lett. 27 (3) (2023) 861–865.
[41] I.S. Gradshteyn, I.M. Ryzhik, Table of integrals, series, and products, in: Academic, seventh ed., 2007.
[42] R.B. Nelsen, An Introduction to Copulas, Springer, 2006.
[43] F. Rostami Ghadi, K.-K. Wong, F. Javier López-Martínez, C.-B. Chae, K.-F. Tong, Y. Zhang, Gaussian Copula approach to the performance analysis of fluid antenna systems, IEEE Trans. Wirel. Commun. 23 (11) (2024) 17573–17585.
[44] M. Abromowitz, I.A. Stegun, Handbook of Mathematical Functions, 1972.