Secrecy Analysis and Optimization of UAV-Assisted Communications with Hybrid SWIPT and Cooperative Jamming

Gaurav K. Pandey, *Student Member, IEEE*, Devendra S. Gurjar, *Senior Member, IEEE*, Suneel Yadav, *Senior Member, IEEE*, Sourabh Solanki, *Member, IEEE*, Juraj Gazda, and Symeon Chatzinotas, *Fellow, IEEE*

***Abstract*—Unmanned aerial vehicles (UAVs) have emerged as a state-of-the-art solution for establishing communication in remote and obstructed areas. However, before UAVs can be integrated into existing communication infrastructure, it is essential to address the energy constraints and security concerns arising from their line-of-sight links. This paper focuses on a UAV-enabled communication system in which a UAV relay facilitates information transfer from the source to the destination nodes when the direct link is heavily shadowed or obstructed. A nearby terrestrial passive eavesdropper can intercept information transmitted through the source-to-UAV and UAV-to-destination links. To address this, we utilize destination-aided cooperative jamming. Additionally, we consider simultaneous wireless information and power transfer (SWIPT) at the UAV to provide the energy required for data transmission. In particular, the UAV utilizes a hybrid-SWIPT technique to harvest energy from the radio-frequency signals. For this setup, we derive accurate expressions of secrecy outage probability and system secrecy throughput (SST) over Beaulieu-Xie distributed channels. Using the SST expression, we formulated an SST maximization problem by jointly optimizing the transmit powers, power allocation, SWIPT coefficients, and UAV's three-dimensional position. The formulated problem is solved using the hybrid heuristic framework, combining continuous genetic and particle swarm optimization algorithms. Numerical results demonstrate the significant enhancement in information secrecy of the system with the proposed hybrid scheme and also provide valuable insights into the system's behavior.**

***Keywords*—Unmanned aerial vehicle, energy harvesting, cooperative destination jamming, Beaulieu-Xie distributed channels, secrecy performance, hybrid heuristic optimization algorithm.**

I. Introduction

Non-terrestrial networks (NTNs), which comprise satellites, high altitude platforms (HAPs), and unmanned aerial vehicles (UAVs), are conventionally employed for civilian applications such as search operations, emergency rescue, agronomic preservation, environmental-based predictions, and traffic surveillance [1]. Moreover, with the evolving beyond fifth-generation (B5G) standards, NTNs are expected to become the future hot spot, especially with the adoption of UAVs, which will be crucial in providing ubiquitous access owing to their flexible mobility and high line-of-sight (LoS) connectivity [2]. In one of the possible application scenarios, UAVs can act as cooperative aerial relays to assist data transmission and provide coverage to ground terminals. While working as aerial relays or base stations, UAVs require considerable energy to perform communication operations. However, size, weight, and power constrain the UAVs from carrying large-sized batteries. Thus, onboard energy limitations affect their flight duration, restraining their operational time [3]. Energy harvesting (EH) methods can be a viable solution to provide the energy needed for data transmission operations and support the onboard batteries. To this end, harvesting the energy from radio-frequency (RF) signals possibly addresses the UAV's power constraints to some extent [4]. They can employ simultaneous wireless information and power transfer (SWIPT) techniques with any of receiver architectures, i.e., time switching (TS) and power-splitting (PS) [5]. Several research works [6]–[8] have employed the RF-EH techniques for energy-constrained UAVs and utilized them for relaying operations in different application scenarios. Specifically, the authors in [6] considered a one-way relaying scheme and employed EH at the relay node. Similarly, the authors in [7] employed an energy-constrained UAV relay to forward the data from the base station to two users by using the non-orthogonal multiple access (NOMA) technique. Additionally, the authors in [8] explored a cognitive network supported by energy-constrained UAVs to enhance offloading efficiency.

In another direction, the aerial links, i.e., air-to-ground (A2G) and ground-to-air (G2A), can become susceptible to security threats because the UAV's dominant LoS can provide better channel conditions to not only the legitimate nodes but also to the eavesdroppers [9]. From the physical layer (PHY) security perspective, the attacks on the UAV-integrated wireless networks can be classified into two scenarios [10]. In particular, the terrestrial malicious nodes can launch eavesdropping/jamming attacks that are more severe to the UAV's A2G link than terrestrial links [11]. In another

Gaurav Kumar Pandey and Devendra Singh Gurjar are with the Department of Electronics and Communication Engineering, National Institute of Technology Silchar, Cachar, Assam, 788010, India (e-mails: {gaurav_rs, dsgurjar}@ece.nits.ac.in).

Suneel Yadav is with the Department of Electronics and Communication Engineering, Indian Institute of Information Technology Allahabad, Prayagraj, Uttar Pradesh, 211015, India (e-mail: suneel@iiita.ac.in).

Sourabh Solanki is with Department of Electronics and Communication Engineering, National Institute of Technology Warangal, India (email: ssolanki@nitw.ac.in).

Juraj Gazda is with the Department of Computer and Informatics, Technical University of Košice, 04200 Košice, Slovakia (e-mail: juraj.gazda@tuke.sk).

Symeon Chatzinotas is with SnT, University of Luxembourg, 1855 Luxembourg City, Luxembourg (emails: symeon.chatzinotas@uni.lu).

scenario, the attackers can exploit the malicious UAV to launch eavesdropping/jamming attacks. In recent years, several PHY security methods, like cooperative jamming, artificial noise (AN) injection, etc., have been introduced to improve the network's security [12]. Many studies have considered the PHY security techniques for UAV-assisted networks with different system configurations [13]–[19]. For example, the authors in [13] adopted NOMA-based UAV-aided model, where aerial jamming and optimal power allocation were utilized for securing the communication. In another work [14], the authors employed dual UAVs to facilitate data transfer and enhance data security via cooperative jamming against a terrestrial eavesdropper. Similarly, the authors in [15] utilized a friendly secondary UAV jammer to transmit the jamming signals to the eavesdropper.

In [16] and [17], the authors maximized the secure computation capacity and secrecy capacity, respectively, using the convex approximation techniques. The authors in [18] leveraged analytical secrecy outage probability (SOP) expressions to ascertain optimal UAV positioning and resource allocation using a hybrid algorithm integrating particle swarm optimization (PSO) with genetic local search features. However, the jamming signals transmitted by the UAVs may interfere with the information signal, making it difficult for legitimate nodes to distinguish between the information and the jamming signal or AN [20]. With this regard, authors in [19], [21], [22] employed destination nodes to transmit jamming signals or AN to confuse the eavesdropper and enhance secrecy performance in UAV communications. In particular, the authors in [19] combined cooperative destination and external UAV jamming schemes.

Recent studies have integrated RF-EH techniques with PHY security in UAV communications to enhance both network longevity and security [21]–[26]. Specifically, the authors in [21] adopted a destination-assisted cooperative jamming scheme and PS-based SWIPT at the amplify-and-forward (AF)-based UAV relay. In another work [22], a full-duplex destination node has been considered that receives the information from UAV and transmits AN to the eavesdroppers simultaneously. Similarly, the authors in [23] utilized WPT and UAV trajectory planning for their considered system model. Whereas, the authors in [24] analyzed the impact of secondary user interference on security in decode-and-forward (DF)-employing multiple UAV-assisted NOMA-based cognitive radio networks. Likewise, the authors in [25] addressed security issues for offloading tasks and control signal transmission in mobile edge computing-assisted UAV communications. Further, the work in [26] focused on the joint minimization of outage probability (OP) and intercept probability (IP) in both links by utilizing their closed-form expressions. The following research gaps exist in the literature mentioned above:

- Many existing studies [13]–[19] have focused on security aspects without providing an integrated framework that improves security and energy efficiency in UAV-based networks.
- Several research works on RF-EH and PHY-security, including [21]–[26], considered either TS or PS-based SWIPT architectures for accomplishing the energy and information transfer via a UAV relay. However, using a hybrid TS-PS SWIPT technique remains unexplored in these studies despite its potential to enhance harvested energy and secrecy performance [27]–[29].
- The works in [21]–[25] primarily focused on addressing security issues in either A2G or G2A links. However, it is essential to secure both A2G and G2A links in UAV communications.
- Most of the recent works like [6]–[8], [13]–[19], [21]–[26] have analyzed the system performance or formulated the optimization problems over free-space path-loss (PL), Rician, Nakagami-m, or Rayleigh fading channels. However, these fading models do not fully capture the diverse propagation characteristics of UAV links, particularly the interplay of LoS and multipath components in A2G and G2A transmissions.

Motivated by the above discussion and existing literature gaps, we utilize RF-EH and cooperative jamming methods for secure and reliable UAV-enabled communications. We present Table I to give an overview of the contributions of this work and compare them with other relevant studies. Specifically, we consider a UAV [1] that harvests the energy from the signal transmitted from source and destination nodes for performing AF-based relaying[2] operations. We adopt a hybrid TS-PS-based SWIPT technique[3] for executing secure information transfer from source to destination node [22]. Moreover, we emphasize the importance of securing communication networks for A2G and G2A links. Thus, we employ destination-based cooperative jamming to distract the eavesdropper in both transmission links. Furthermore, we utilize Beaulieu-Xie (Be-Xi) fading distribution to model the channels between the communicating nodes [31]. Utilizing this, we derive accurate SOP and system secrecy throughput (SST) expressions over the Be-Xi distributed channels to analyze security performance with various system and channel parameters. We also obtain the asymptotic SOP in a high signal-to-noise ratio (SNR) regime to get key insights into the system's performance. Next, we utilize the SST expression to formulate the SST maximization problem by jointly optimizing transmit powers, power allocation, SWIPT parameters, and UAV locations. The non-convex nature and tightly coupled variables make the optimization problem intractable. Therefore, we employ a hybrid heuristic algorithm, i.e., PSO and continuous genetic algorithms (CGA) to handle the complex multi-variable problems efficiently. To

[1]The propulsion energy consumption of U_R is significantly higher than the energy utilized for data transmission. Based on the commonly adopted assumption in the literature [21], [22], [24], [25], the onboard battery of U_R powers the propulsion mechanism, whereas the harvested energy at U_R is utilized for information transmission [24], [25].

[2]Although both AF and DF are widely used relaying techniques in cooperative networks, we utilize AF relaying because it offers lower complexity than DF relaying. Moreover, we employ AF-based UAV relaying so that U_R can amplify the jamming noise received in the first IT phase and broadcast it in the second IT phase to degrade the SINR at the eavesdropper.

[3]The hybrid TS-PS-based SWIPT technique employs both TS and PS protocols, which leads to increased complexity in the receiver architecture [27]–[30]. However, this technique allows for a significant increase in the harvested power at U_R during the first two phases, which improves the system's security performance, as depicted in Section V. Thus, the increased complexity can be compensated by the enhanced performance of the hybrid TS-PS model compared to separate TS and PS-based receiver architectures.

TABLE I
COMPARISON OF PROPOSED WORK WITH RELEVANT LITERATURE

Works	System Model				Fading Model	SWIPT Protocol	Analytical Assessment	Optimizing	
	Aerial Links	PHY Security Technique	RF-EH	EH Node				System Parameters	UAV Attributes
[8]	A2G, G2A	×	✓	UAV	Free-space PL	TS	×	✓	⊙
[13]	A2G	Aerial jamming	×	×	Probabilistic model, Nakagami-m	×	SOP, COP	×	⊙
[15]	A2G	Aerial jamming	×	×	Free-space PL	×	×	✓	✓
[16]	G2A	Ground jamming	×	×	Free-space PL	×	×	✓	✓
[17]	A2G	×	×	×	Free-space PL	×	×	✓	✓
[18]	A2G	×	✓	×	Probabilistic model	×	×	×	✓
[24]	A2G	×	✓	UAVs	Rayleigh fading	TS	OP, leakage probability	⊙	⊙
[25]	G2A	Ground jamming	✓	UAV	Rayleigh fading	TS	×	✓	✓
[26]	A2G	AN injection	✓	UAV	Rician fading, Rayleigh fading	TS	OP, IP	⊙	⊙
Our work	A2G, G2A	Destination jamming	✓	UAV	Elevation angle-dependent PL, Beaulieu-Xie fading	Hybrid, TS-PS	SOP, SST, asymptotic SOP	✓	✓

✓ Covered ⊙ Partially covered × Not covered

the best of the authors' knowledge, no work has yet analyzed the security performance and optimized the security metrics in UAV-enabled communications with destination jamming and hybrid TS-PS-based SWIPT considering such a scenario. A brief overview of the paper's significant contributions is as follows:

- We propose a secure and energy-efficient UAV-enabled communication framework incorporating hybrid TS-PS-based SWIPT and destination-based cooperative jamming.
- We model the A2G and G2A communication links between the communicating nodes using the Be-Xi fading distribution and elevation angle-dependent PL.
- By using the described channel model, we derive closed-form expressions for the SOP and SST and provide asymptotic SOP analysis in a high SNR regime.
- We formulate an SST maximization problem by optimizing transmit powers, power allocation, SWIPT parameters, and UAV placement while considering the security and practical constraints.
- Then, we offer a hybrid optimization framework, combining CGA and PSO algorithms, to efficiently solve the non-convex optimization problem.
- Lastly, we assess the effectiveness of our proposed scheme by comparing it with established benchmark schemes and provide valuable insights for efficient system design.

A. Organization

The rest of the paper is organized as follows: Section II describes the proposed system and channel models, then discusses the considered transmission scheme and obtains the expressions of end-to-end SNRs. Section III examines the system performance in terms of exact and asymptotic expressions of SOP and SST. In Section IV, we utilize the AO algorithm to evaluate the optimum values for power allocation, SWIPT parameters, and UAV locations. Then, the numerical and simulation results are presented in Section V. Finally, Section VI concludes the paper.

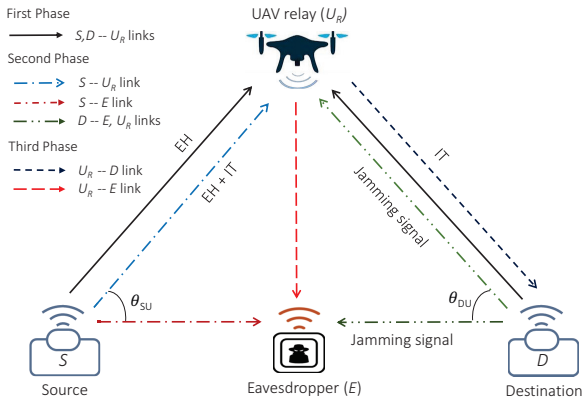

Fig. 1. UAV-enabled communication with hybrid SWIPT and cooperative destination jamming.

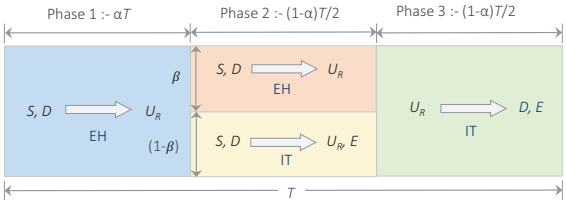

Fig. 2. Transmission block of the considered system.

Notations: The probability, probability density function (PDF), and cumulative distribution function (CDF) of a random variable X are denoted by $\Pr[\cdot]$, $f_X(\cdot)$, and $F_X(\cdot)$, respectively. $\mathcal{I}_\nu(\cdot)$ and $\mathcal{K}_\nu(\cdot)$ are the modified Bessel function of the first kind and second kind of νth order, respectively and the Marcum-Q function is denoted by $Q_\nu(a,b)$. The expectation operator is represented as $\mathbb{E}[\cdot]$ and $\Gamma(\cdot)$ denotes the complete gamma function.

II. System Model and Channel Model

A. System Model

We consider a UAV-assisted relaying scheme with destination jamming to provide a secure and reliable communication

between two terrestrial nodes as illustrated in Fig. 1. Here, the source (S) cannot directly transmit the information signals to the destination (D) due to obstacles or heavy shadowing. Therefore, an energy-constrained UAV relay (U_R) provides assistance for transmitting confidential information of S to D in the presence of a terrestrial eavesdropper (E). For the sake of analytical treatment in performing the secrecy analysis, we consider a linear EH model at U_R [13], [14], [19], [22], [32]. The nodes S, D, and E are fixed on the ground, whereas the U_R hovers at $\mathbf{H}$ height to provide relay assistance to terrestrial nodes. All nodes are assumed to be equipped with a single antenna, aligning with practical considerations in UAV communications and consistent with prior research [8], [11], [13], [17], [22], [26].

Both operations, i.e., EH and confidential information transmission (IT) from S to D, are performed in three phases, as depicted in Fig. 2. Specifically, the first phase refers to the EH phase of αT duration in which the energy-constrained U_R employs TS protocol to harvest the energy from the signal received from S and D. Whereas, in the second phase, which refers to the first IT phase of $(1-\alpha)T/2$ duration, the U_R utilizes a fraction of the received signal power for the EH using PS protocol. Then U_R uses the remaining fraction of the signal power for information processing and broadcasting in the next phase. Considering a more severe eavesdropping threat, we assume that the E is present in the vicinity of both S and D so that it can wiretap the information in both IT phases. Thus, we adopt a destination jamming scheme to ensure security in the first IT phase, wherein the D broadcasts the jamming signal to E and U_R. In the third phase, which refers to the second IT phase, U_R adopts AF relaying protocol for forwarding the scaled version of the signal received in the first IT phase.

B. Channel Model

We assume a block fading scenario, where the channel coefficients between two involved nodes, denoted by h_{ij} $\forall$ $(ij)\in\{(SU),(DU),(SE),(DE),(UE)\}$, remain constant for the entire block duration of T (comprising of one EH phase and two IT phases). Accurate channel modeling plays a crucial role in characterizing more specific practical scenarios that account for different wireless fading channels. Nakagami-m distribution with fading severity parameter of m and average power Ω can be used to model various fading scenarios by varying m value [33]. On the other side, Rician distribution with the shape parameter, $K=\frac{\mathcal{V}^2}{2\sigma^2}$, and scale parameter, $\Omega=\mathcal{V}^2+2\sigma^2$, can be exploited to model scenarios with LoS components. Likewise, Be-Xi fading distribution can be used to model LoS and non-line-of-sight (NLoS) scenarios, i.e., both specular and diffused scattering components [31], [34]. Motivated by this, we consider that the channels between two communicating nodes follow Be-Xi distribution, whose PDF and CDF are given as

$$f_X(x;m,\lambda,\Omega)=\frac{2me^{-\frac{m}{\Omega}(\lambda^2+x^2)}}{\Omega\lambda^{m-1}}x^m\mathcal{I}_{m-1}\left(\frac{2m\lambda}{\Omega}x\right), \quad (1)$$

$$F_X(x;m,\lambda,\Omega)=1-Q_m\left(\sqrt{\frac{2m}{\Omega}}\lambda,\sqrt{\frac{2m}{\Omega}}x\right), \quad (2)$$

where λ^2 represents the power of LoS components, m is the shape parameter and the power of the NLoS component is given by Ω, where $\Omega=\mathbb{E}[X^2]$ [31]. $\mathcal{I}_\nu(x)$ and $Q_\nu(a,b)$ are expressed as [35]

$$\mathcal{I}_\nu(x)=\left(\frac{x}{2}\right)^\nu\sum_{q=0}^{\infty}\frac{\left(\frac{x^2}{4}\right)^q}{q!\,\Gamma(\nu+q+1)}, \quad (3)$$

$$Q_\nu(a,b)=\sum_{p=0}^{\infty}e^{-\frac{a^2}{2}}\frac{\left(\frac{a^2}{2}\right)^p}{p!}\sum_{k=0}^{p+\nu-1}e^{-\frac{b^2}{2}}\frac{\left(\frac{b^2}{2}\right)^k}{k!}. \quad (4)$$

Additionally, we focus on considering more practical scenarios where surrounding obstacles like buildings or trees may block the LoS link between U_R and terrestrial nodes. Thus, we adopt the elevation angle-dependent PL model that considers the PL between the communicating nodes as a function of θ_{ij}, where $\theta_{ij}=\arctan(\mathbf{H}/r_{ij})$, $\forall$ $(ij)\in\{(SU),(DU),(SE),(DE),(UE)\}$ is the angle and $r_{ij}=\sqrt{(\mathbf{x}_i-\mathbf{x}_j)^2+(\mathbf{y}_i-\mathbf{y}_j)^2}$ is the horizontal distance between the communicating nodes. In the same line, the distance between U_R and terrestrial nodes are given as $d_{Uk}=\sqrt{(\mathbf{x}_U-\mathbf{x}_k)^2+(\mathbf{y}_U-\mathbf{y}_k)^2+\mathbf{H}^2}$, where $\mathbf{q}_U=(\mathbf{x}_U,\mathbf{y}_U,\mathbf{H})$ and $\mathbf{w}_k=(\mathbf{x}_k,\mathbf{y}_k,0)$, $\forall$ $k\in\{S,D,E\}$ are Cartesian coordinates of U_R's and terrestrial nodes' location. The distances between the terrestrial nodes are given as $d_{SE}=r_{SE}$ and $d_{DE}=r_{DE}$. The adopted PL model is generic and efficiently captures the aerial and terrestrial propagation by considering elevation angle and distance between the nodes. It is important to note that the signals transmitted in the terrestrial links, i.e., S–E and D–E can undergo complete non-line of sight (NLoS) propagation due to $\theta_{SE}=\theta_{DE}=0$ (since, $\mathbf{H}=0$), corresponding to heavily shadowed fading scenarios. However, the PL in the aerial links is the function of $\theta_{ij}\in\{0,90\}$ (in degrees). The large scale attenuation between the nodes i and j is given as $L_{ij}=|d_{ij}|^{-\alpha_{ij}}$, where α_{ij} denotes the PL exponent, obtained as $\alpha_{ij}=\alpha_{\text{NLoS}}+\left(\frac{\alpha_{\text{LoS}}-\alpha_{\text{NLoS}}}{1-\omega_1 e^{-\omega_2(\theta_{ij}-\omega_1)}}\right)$, where α_{LoS} and α_{NLoS} are the PL exponents for complete LoS and NLoS links, respectively and ω_1, ω_2 are scenario-specific constants [21].

C. Energy Harvested at the UAV

Several studies [6]–[8], [24], [25] have investigated energy-constrained UAVs that utilize RF-EH technique to harvest energy and subsequently use it for data transmission operations. Similar to these works, U_R harvests the energy from the RF signals received from S as well as from the jamming signal transmitted from the D by using the TS approach in the EH phase. The energy harvested at U_R in this phase is given as

$$\mathcal{E}_{\text{H}}^{\text{TS}}=\eta_1\alpha T\left(P_S L_{SU}|h_{SU}|^2+P_D L_{DU}|h_{DU}|^2\right), \quad (5)$$

where η_1 denotes the energy conversion efficiency of the linear EH circuit at U_R, where $0<\eta_1<1$. The TS ratio (TSR), denoted as $0<\alpha<1$, decides the time allocated for EH and IT. Unlike other related works, a more generalized scenario is considered in which the terrestrial E can exploit the broadcasted information in both the IT phases and pose a more detrimental threat. Thus, in the first IT phase, S transmits

the confidential information to U_R, and simultaneously, D employs cooperative jamming and broadcasts the jamming signal in order to degrade the SINR of the E. The signal received by U_R is given as

$$y_{SU} = \sqrt{P_S L_{SU}} h_{SU} x_S + \sqrt{P_D L_{DU}} h_{DU} x_D + n_{\mathrm{U}}, \quad (6)$$

where x_S and x_D are the unit-energy symbols and P_S and P_D are the transmit power of S and D, respectively. The noise component n_{U} is modeled as additive white Gaussian noise (AWGN), i.e., $n_{\mathrm{U}} \in \mathcal{CN}(0, N_0)$. Additionally, $P_S = \epsilon P_T$ and $P_D = (1-\epsilon)P_T$, where P_S and P_D satisfy the condition, i.e., $P_S + P_D = P_T$. Here, ϵ is the power allocation factor (PAF), satisfying $0 < \epsilon < 1$. Next, U_R employs PS protocol to harvest energy from the received signal. The received signal power is split into two parts, i.e., $(\sqrt{\beta} y_{\mathrm{SU}})^2$ is used for EH and $(\sqrt{(1-\beta)} y_{\mathrm{SU}})^2$ is utilized for information transmission, where $0 < \beta < 1$ represents the power splitting ratio (PSR). Thus, the energy harvested at U_R is given as

$$\mathcal{E}_{\mathrm{H}}^{\mathrm{PS}} = \frac{\eta_2 \beta (1-\alpha) T}{2} \left(P_S L_{SU} |h_{SU}|^2 + P_D L_{DU} |h_{DU}|^2 \right), \quad (7)$$

where $0 < \alpha < 1$ denotes the time switching ratio (TSR) that controls the time allocated for the EH and IT, η_2 denotes the energy conversion efficiency. We assume that the total energy harvested in the first two phases is utilized for relaying the information signal to D. The total power available at U_R for relaying the signal can be expressed as

$$\mathcal{P}_{\mathrm{H}}^{\mathrm{Tot}} = \left(\frac{2\eta_1 \alpha}{1-\alpha} + \eta_2 \beta \right) \left(P_S L_{SU} |h_{SU}|^2 + P_D L_{DU} |h_{DU}|^2 \right). \quad (8)$$

We assume that the total energy that U_R harvests by employing both TS and PS-based SWIPT protocols is fully utilized to relay the information to D.

Remark 1: It is important to note that:

- *A system model with TS-based SWIPT architecture can be obtained from the hybrid TS-PS-based model by substituting $\beta = 0$ in (8).*
- *A system model with PS-based SWIPT architecture can be acquired from the hybrid TS-PS-based model by setting $\alpha = 0$ in (8) [21].*
- *A system model with TS-PS-based SWIPT architecture without cooperative jamming can be obtained by substituting $\epsilon = 1$, i.e., all the power is allocated for IT and the jamming power at the destination node, $P_D = 0$.*
- *These three techniques are employed as baseline methods in Section V, which compares the system's security performance with the proposed scheme.*

D. Instantaneous Signal-to-Interference-plus-Noise Ratios

In the first IT phase, after applying PS-based SWIPT, the remaining information signal received at U_R is expressed as

$$y_{SU}^{(\mathrm{rem})} = \sqrt{(1-\beta) P_S L_{SU}} h_{SU} x_S + \sqrt{(1-\beta) P_D L_{DU}} h_{DU} x_D + \sqrt{(1-\beta)} n_{\mathrm{U}} + n_{\mathrm{CN}}, \quad (9)$$

where n_{CN} represents RF to baseband conversion noise and is modeled as AWGN, i.e., $n_{\mathrm{CN}} \in \mathcal{CN}(0, N_0)$. At the same time, the signal received at E is given as $y_{SE} = \sqrt{P_S L_{SE}} h_{SE} x_S + \sqrt{P_D L_{DE}} h_{DE} x_D + n_{\mathrm{E}}$, where $n_{\mathrm{E}} \in \mathcal{CN}(0, N_0)$ is the noise component, which is modeled as AWGN. Therefore, the instantaneous signal-to-interference-plus-noise ratio (SINR) at E in the first phase is expressed as

$$\gamma_{SE} = \frac{P_S L_{SE} |h_{SE}|^2}{P_D L_{DE} |h_{DE}|^2 + N_0}. \quad (10)$$

In the second IT phase, U_R applies an AF relaying to broadcast the signal by scaling the remaining information signal, as obtained in (9), with the amplification factor $\mathcal{G}$. Thus, the information received at D and E are denoted as

$$y_{U,l}^{\mathrm{BC}} = \underbrace{\mathcal{G} \sqrt{(1-\beta) P_S L_{SU} L_{Ul}} h_{SU} h_{Ul} x_S}_{\text{Information signal from } S-l} + \underbrace{\mathcal{G} \sqrt{(1-\beta) P_D L_{DU} L_{Ul}} h_{DU} h_{Ul} x_D}_{\text{Jamming signal from } D} + \underbrace{\mathcal{G} (\sqrt{(1-\beta)} n_{\mathrm{U}} + n_{\mathrm{CN}}) \sqrt{L_{Ul}} h_{Ul} + n_l}_{\text{AWGN}}, \quad (11)$$

for $l \in \{D, E\}$, where $n_l \in \mathcal{CN}(0, N_0)$ represents the AWGN at D and E. The amplification factor $\mathcal{G}$ is approximated as

$$\mathcal{G}^2 = \frac{\mathcal{P}_{\mathrm{H}}^{\mathrm{Tot}}}{(1-\beta)(P_S L_{SU} |h_{SU}|^2 + P_D L_{DU} |h_{DU}|^2 + N_0) + N_0}. \quad (12)$$

Since the destination receives the scaled version of its prior known jamming signal transmitted in the first IT phase, it can neutralize its signal by conducting complete self-interference cancellation. Hence, the interference from the jamming signal will be removed from (11) for D. However, this interference term will be present in (11) for E. The SINR at D and E can be obtained by substituting the values of $\mathcal{G}$ and performing some mathematical simplifications. The SINR at D and E can be expressed as in (13) and (14), respectively. Additionally, considering the high/moderate SNRs, we assume $\varphi \simeq 0$ in (13) and (14) for simplicity of the results, where $\varpi = \left(\frac{2\eta_1 \alpha}{1-\alpha} + \eta_2 \beta \right)$, $\varphi = \frac{N_0^2}{(P_S L_{SU} |h_{SU}|^2 + P_D L_{UD} |h_{UD}|^2)}$.

III. Performance Analysis

In this section, we obtain the accurate expressions of SOP and SST to analyze the secrecy performance of the proposed system model.

A. Secrecy Outage Probability (SOP) Analysis

We adopt a precise secrecy outage formulation for the proposed system model that efficiently acquires the probability that the transmitted information fails to achieve perfect secrecy [36]. We use a well-known Wyner's encoding technique wherein an encoder selects the codeword transmission rate, $\mathcal{R}_b$ and the confidential data transmission rate $\mathcal{R}_c$ for the information transmission from S to D through the relaying U_R [37]. The rate difference, i.e., $\mathcal{R}_d = \mathcal{R}_b - \mathcal{R}_c$, accounts for the cost of secured information transmission against E [38], [39]. Further, E can perform the selection combining (SC) scheme over the signal copies received in two phases, thereby launching a more severe security threat [19], [21]. Thus, for any transmitted information, the secrecy of the

$$\gamma_{SD} = \frac{\varpi(1-\beta)P_S L_{SU} L_{UD} |h_{SU}|^2 |h_{UD}|^2}{\varpi(2-\beta)L_{UD}|h_{UD}|^2 N_0 + (1-\beta)N_0 + \varphi}, \tag{13}$$

$$\gamma_{UE} = \frac{\varpi(1-\beta)P_S L_{SU} L_{UE} |h_{SU}|^2 |h_{UE}|^2}{\varpi(1-\beta)P_D L_{DU} L_{UE} |h_{DU}|^2 |h_{UE}|^2 + (1-\beta)N_0 + \varpi(2-\beta)L_{UE}|h_{UE}|^2 N_0 + \varphi}, \tag{14}$$

information is in outage if the instantaneous capacity at the E, i.e., $\mathcal{C}_E$ is higher than $\mathcal{R}_d$. Here, $\mathcal{C}_E = \frac{(1-\alpha)}{2}\log_2(1+\gamma_E^{\text{SC}})$, where γ_E^{SC} is the resultant SINR at the E after SC operation. Mathematically, the SOP can be formulated as

$$\mathcal{P}_{\text{sop}} = \Pr[\mathcal{C}_E > \mathcal{R}_d] = \Pr[\gamma_E^{\text{SC}} > \delta_d], \tag{15}$$

where $\delta_d = \left(2^{2\mathcal{R}_d/(1-\alpha)} - 1\right)$. Now, we expand the SC condition for E, and reform $\mathcal{P}_{\text{sop}}$ as

$$\begin{aligned}\mathcal{P}_{\text{sop}} &= \Pr[\max(\gamma_{SE}, \gamma_{UE}) > \delta_d] \\ &= 1 - \underbrace{\Pr[\gamma_{SE} \le \delta_d]}_{\triangleq \mathcal{P}_1} \times \underbrace{\Pr[\gamma_{UE} \le \delta_d]}_{\triangleq \mathcal{P}_2}.\end{aligned} \tag{16}$$

In the following Lemmas, we obtain the expressions of $\mathcal{P}_1$ and $\mathcal{P}_2$, given in (16), by substituting different SNR expressions and utilizing the CDFs and PDFs of Be-Xi distribution given in (1) and (2).

Lemma 1: The expression of $\mathcal{P}_1$ in (16) can be given as

$$\begin{aligned}\mathcal{P}_1 = 1 - &\sum_{l=0}^{\infty}\sum_{k=0}^{l+m_{SE}-1}\sum_{c=0}^{C}\sum_{s=0}^{k}\binom{k}{s}\left(\frac{m_{SE}}{\Omega_{SE}}\right)^{l+k} \\ &\times \frac{A^s B^{k-s}\lambda_{se}^{2i}\,\lambda_{de}^{2c}\,\Gamma(C+c)\,(C)^{1-2c}}{l!\;k!\;\Gamma(c+1)\;\Gamma(C-c+1)\;\Gamma(c+m_{DE})} \\ &\times e^{-\left(\frac{m_{DE}}{\Omega_{DE}}\lambda_{DE}^2\right)} e^{-\left(\frac{m_{SE}}{\Omega_{SE}}(\lambda_{SE}^2+B)\right)}\left(\frac{m_{DE}}{\Omega_{DE}}\right)^{m_{DE}+2c} \\ &\times \left(\frac{\Gamma(m_{DE}+c+s)}{\left(\frac{m_{DE}}{\Omega_{DE}} + A\frac{m_{SE}}{\Omega_{SE}}\right)^{m_{DE}+c+s}}\right).\end{aligned} \tag{17}$$

where $A = \frac{P_D L_{DE}\delta_d}{P_S L_{SE}}$ and $B = \frac{N_0\delta_d}{P_S L_{SE}}$.

Proof 1: Please see Appendix A for the proof.

Lemma 2: The expression of $\mathcal{P}_2$ in (16) can be given as

$$\begin{aligned}\mathcal{P}_2 = 1 - &\sum_{r=0}^{\infty}\sum_{\theta=0}^{\phi}\sum_{z=0}^{Z}\sum_{q=0}^{r+m_{SU}-1}\sum_{g=0}^{q}\sum_{l=0}^{g}\binom{g}{q}\binom{d}{g}\frac{\lambda_{SU}^{2r}\,\lambda_{UE}^{2\theta}}{r!\;q!} \\ &\times \left(\frac{m_{SU}}{\Omega_{SU}}\right)^{q+r}\left(\frac{m_{DU}}{\Omega_{DU}}\right)^{m_{DU}+2z}\left(\frac{a_2 m_{SU}\Omega_{UE}}{m_{UE}\Omega_{SU}}\right)^{\frac{m_{UE}-l+\theta}{2}} \\ &\times e^{-\left(\frac{m_{UE}}{\Omega_{UE}}\lambda_{UE}^2\right)}\frac{\Gamma(\phi+\theta)(\phi)^{1-2\theta}\lambda_{DU}^{2z}}{\Gamma(\theta+1)\Gamma(\phi-\theta+1)\Gamma(m_{UE}+\theta)} \\ &\times e^{-\left(\frac{m_{DU}}{\Omega_{DU}}\lambda_{DU}^2\right)}\frac{2\;a_1^{q-g}a_2^{l}a_3^{g-l}\Gamma(Z+z)(Z)^{1-2z}}{\Gamma(z+1)\Gamma(Z-z+1)\Gamma(m_{DU}+z)} \\ &\times e^{-\left(\frac{m_{SU}}{\Omega_{SU}}(\lambda_{SU}^2+a_3)\right)}\frac{\Gamma(m_{DU}+z+q-g)}{\left(\frac{m_{SU}}{\Omega_{SU}}+a_1\frac{m_{DU}}{\Omega_{DU}}\right)^{m_{DU}+z+q-g}} \\ &\times \left(\frac{m_{UE}}{\Omega_{UE}}\right)^{m_{UE}+2\theta}\mathcal{K}_{(m_{UE}-l+\theta)}\left(2\sqrt{\frac{a_2 m_{SU} m_{UE}}{\Omega_{SU}\Omega_{UE}}}\right).\end{aligned} \tag{18}$$

where $a_1 = \frac{(\delta_d P_D L_{DU})}{(P_S L_{SU})}$, $a_2 = \frac{(\delta_d N_0)}{(\varpi P_S L_{SU} L_{UE})}$ and $a_3 = \frac{(\delta_d(2-\beta)N_0)}{((1-\beta)P_S L_{SU})}$.

Proof 2: Please see Appendix B for the proof.

Finally, the overall SOP expression can be obtained by substituting the expressions of $\mathcal{P}_1$ and $\mathcal{P}_2$ given in (17) and (18) into (16).

Remark 2: From the SOP analysis, we can have the following observations.

- *The proposed model provides a generalized model for the presence of E, considering that they can intercept the signal from A2G and G2A links. However, in specific scenarios, as deemed in [21]–[25], where E can be present only in one of the links, the generalized condition can be simplified by considering either γ_{SE} or γ_{UE} in (16), depending on the framework.*
- *From (17), we see that B consists of SNR term, i.e., $B = \frac{\delta_d}{\rho_T \epsilon L_{SE}}$, where $\rho_T = \frac{P_T}{N_0}$ is the transmit SNR. This implies that $B^{k-s}e^{-\frac{m_{SE}}{\Omega_{SE}}B} = \left(\frac{\delta_d}{\rho_T\epsilon L_{SE}}\right)^{k-s}e^{-\frac{m_{SE}}{\Omega_{SE}}\frac{\delta_d}{\rho_T\epsilon L_{SE}}}$ and $l \in \{0,\infty\}$, decreases rapidly because of the dominance of $\left(\frac{1}{\rho_T}\right)^{k-s}$, for the given range of $k \in \{0, l+m_{SE}-1\}$, $s \in \{0,k\}$. Consequently, the SOP increases quickly and approaches to 1 for sufficiently large ρ_T, irrespective of the other involved system and channel parameters, as also verified in Section V.*
- *It is also observed from (17) that the terms A and B are proportional to δ_d that consists of time-switching parameter, α, i.e., $A, B \propto \delta_d = 2^{\frac{2\mathcal{R}_d}{1-\alpha}} - 1$. Accordingly, SOP is proportional to $\frac{A^s B^{k-s}e^{-\frac{m_{SE}}{\Omega_{SE}}B}}{\left(\frac{m_{DE}}{\Omega_{DE}}+A\frac{m_{SE}}{\Omega_{SE}}\right)^{m_{DE}+c+s}} \triangleq \frac{\delta_d^k e^{-\frac{m_{SE}}{\Omega_{SE}}\delta_d}}{\left(\frac{m_{DE}}{\Omega_{DE}}+\delta_d\frac{m_{SE}}{\Omega_{SE}}\right)^{m_{DE}+c+s}}$, for the given range of s, c, k. From this, we can infer that the above term is dominated by δ_d^k which increases with increase in α, and consequently SOP decreases. The impact of α on the SOP performance is also shown numerically in Section V.*
- *Likewise, we can also analytically demonstrate the impact of various other involved parameters on (17). We can also make similar observations about (18).*
- *Importantly, (17) and (18) consist of infinite series terms which converge quickly to achieve a fair accuracy in obtaining the final value.*

B. Asymptotic SOP Analysis

In this section, we perform the asymptotic SOP analysis in the high SNR regime to study the impact of channel and system parameters on the system's secrecy diversity behavior. By following the similar steps as adopted in Appendix A and

Appendix B to obtain $\mathcal{P}_1$ and $\mathcal{P}_2$, the expressions of asymptotic SOP can be easily obtained. Therefore, by substituting $\frac{P_T}{N_0} \to \infty$ into (30) and (38) with P_S/P_D being held constant, the asymptotic expressions can be obtained, which are denoted as $\mathcal{P}_1^{\text{asym}}$ and $\mathcal{P}_2^{\text{asym}}$ and given by

$$\mathcal{P}_1^{\text{asym}} = 1 - \sum_{l=0}^{\infty} \sum_{k=0}^{l+m_{SE}-1} \sum_{c=0}^{C} \left(\frac{m_{SE}}{\Omega_{SE}}\right)^{l+k} \left(\frac{m_{DE}}{\Omega_{DE}}\right)^{m_{DE}+2c} \times e^{-\left(\frac{m_{DE}}{\Omega_{DE}}\lambda_{DE}^2 + \frac{m_{SE}}{\Omega_{SE}}\lambda_{SE}^2\right)} \frac{\Gamma(m_{DE}+c)}{\left(\frac{m_{DE}}{\Omega_{DE}} + A\frac{m_{SE}}{\Omega_{SE}}\right)^{m_{DE}+c}} \times \frac{A^k \lambda_{SE}^{2i}\, \lambda_{DE}^{2c}\, \Gamma(C+c)\, (C)^{1-2c}}{l!\; k!\; \Gamma(c+1)\; \Gamma(C-c+1)\; \Gamma(c+m_{DE})}. \tag{19}$$

$$\mathcal{P}_2^{\text{asym}} = 1 - \sum_{r=0}^{\infty} \sum_{z=0}^{Z} \sum_{q=0}^{r+m_{SU}-1} \frac{\lambda_{SU}^{2r}\, \lambda_{DU}^{2z}}{r!\; q!} \left(\frac{m_{DU}}{\Omega_{DU}}\right)^{m_{DU}+2z} \times e^{-\left(\frac{m_{SU}}{\Omega_{SU}}\lambda_{SU}^2 + \frac{m_{DU}}{\Omega_{DU}}\lambda_{DU}^2\right)} \frac{\Gamma(m_{DU}+z+q)}{\left(\frac{m_{SU}}{\Omega_{SU}} + a_1\frac{m_{DU}}{\Omega_{DU}}\right)^{m_{DU}+z+q}} \times \left(\frac{m_{SU}}{\Omega_{SU}}\right)^{q+r} \frac{a_1^q \Gamma(Z+z)(Z)^{1-2z}}{\Gamma(z+1)\Gamma(Z-z+1)\Gamma(m_{DU}+z)}. \tag{20}$$

On invoking (19) and (20) in (16), we can obtain the asymptotic SOP expression.

Remark 3: It can be observed from (19) and (20) that the asymptotic SOP expression is independent of P_T. As a result, the asymptotic SOP curves may exhibit the saturation floor with varying SNR values, as highlighted in Figs. 4 and 5 in Section V.

C. System Secrecy Throughput (SST)

For the considered delay limited secured information transmission via U_R relaying network, SST can be obtained in terms of SOP and the confidential data transmission rate $\mathcal{R}_c$ [40]. Thus, for the proposed transmission scheme, the expression of SST is given as

$$\mathcal{T}_{\text{sys}}^{\text{sec}} = \frac{(1-\alpha)}{2}(1 - \mathcal{P}_{\text{sop}})\mathcal{R}_c, \tag{21}$$

where $\mathcal{R}_c$ is in bps/Hz. Invoking (17) and (18) into (21), one can get the final expression of SST. Our primary goal is to maximize the SST of the network while adhering to security constraints. The following section will formulate the SST maximization problem using the final SST expressions derived in equation (21).

IV. SST Maximization Problem and Proposed Hybrid Framework

In this section, we focus on joint resource allocation and U_R's optimal placement to maximize the SST for our considered system. Specifically, the SST maximization problem is formulated by optimizing various system parameters such as TSR, PSR, and PAF (α, β, ϵ), transmit powers of S and D (P_S, P_D), and U_R's 3D location ($\mathbf{q}_U$).

A. Problem Formulation

We formulate the SST maximization problem (P1), utilizing the final expression of SST in (21), as

$$(\text{P1}): \max_{\substack{\alpha,\beta,\epsilon,\\ P_S,P_D,\mathbf{q}_U}} \quad \mathcal{T}_{\text{sys}}^{\text{sec}} \tag{22a}$$

$$\textbf{s.t.} \quad \mathcal{P}_{\text{sop}} \le \gamma_s, \tag{22b}$$

$$0 \le P_S \le P_S^{\max}, \tag{22c}$$

$$0 \le P_D \le P_D^{\max}, \tag{22d}$$

$$0 \le \alpha < 1,\ 0 \le \beta < 1,\ 0 < \epsilon \le 1, \tag{22e}$$

$$\mathbf{q}_U^{\min} \le \mathbf{q}_U \le \mathbf{q}_U^{\max}, \tag{22f}$$

where $\mathbf{q}_U^{\min}$ and $\mathbf{q}_U^{\max}$ are the minimum and maximum flying limits of U_R, given by $(\mathbf{x}_U^{\min}, \mathbf{y}_U^{\min}, H^{\min})$ and $(\mathbf{x}_U^{\max}, \mathbf{y}_U^{\max}, H^{\max})$, respectively. Moreover, $P_S^{\max}$ and $P_D^{\max}$ represent the maximum transmit powers of S and D, respectively. The constraints of the formulated problem (P1) are described as: (22b) ensures the confidentiality of information by keeping the $\mathcal{P}_{\text{sop}}$ below a threshold value, given by γ_s. Furthermore, (22c) and (22d) set constraints on the transmit powers of both S and D. The constraints on the system parameters ϵ, α, and β are defined in equation (22e). Whereas the constraint defined in (22f) corresponds to restrictions on the positions of U_R. For convenience, we denote the optimization variables set as $\mathbb{V}$, which includes α, β, ϵ, P_S, P_D, and the tuples ($\mathbf{q}_U$). It can be observed that the formulated optimization problem (P1) exhibits non-convex behavior characterized by multiple local maxima. Moreover, the high-dimensional continuous search space with tightly coupled optimizing variables makes it difficult to tackle. Consequently, we utilize a hybrid heuristic algorithm, combining PSO and CGA to solve (P1) in the following subsection.

B. Evolutionary and Swarm Intelligence-based Algorithm

In this section, we utilize a hybrid algorithm that efficiently solves (P1) by combining the PSO's fast convergence with the strong exploratory capabilities of CGA. Now, we provide a detailed description of the proposed hybrid framework, including the formation of search space, penalty function, convergence, and computational complexity analysis.

1) Outline of Hybrid CGA-PSO-based Secure Framework: The CGA algorithm is an improved version of GA, which can effectively manage a large number of continuous variables. Wherein, the chromosome is represented as a real valued vector, therefore the Ψth chromosome in the $\mathcal{G}$th generation is given by

$$\mathbb{V}(\mathcal{G})_\Psi = [\alpha, \beta, \epsilon, [\mathbf{q}_U]_{1\times 3}, P_S, P_D], \tag{23}$$

where the dimension of $\mathbf{q}_U$ is (1×3).

Remark 4: The considered model can be extended by considering N number of UAVs, which have the dimension of $\boldsymbol{q}_{U_n}, \forall n \in N$ as $(N \times 3)$. This indicates that when a new solution candidate utilizes more UAVs than the previous one, an additional UAV position can be incorporated into the chromosome and optimized accordingly. To facilitate an efficient heuristic search, the candidate chromosome $\mathbb{V}(\mathcal{G})_\Psi$ can be

modified by setting the dimension N of the matrix $[\boldsymbol{q}_U]_{N\times 3}$ to its upper limit, denoted as N^{max}. Consequently, (23) *can be transformed as* $\mathbb{V}(\mathcal{G})_\Psi = [N, \alpha, \beta, \epsilon, [\boldsymbol{q}_U]_{N^{max}\times 3}, P_S, P_D]$.

The algorithm initializes by randomly generating chromosomes with the population $\mathbb{V}(0)_\Psi$. Each chromosome is evaluated using the objective function described in (22a). Promising chromosomes are chosen for reproduction during the selection phase to maintain the population size ζ. In the crossover stage, the majority of chromosomes undergo pairing and recombination at a predefined crossover rate (R_{co}) to produce offspring. Specifically, when the hybrid CGA-PSO algorithm selects a pair of chromosomes, $\mathbb{V}(\mathcal{G})_{\check{m}}$ and $\mathbb{V}(\mathcal{G})_{\check{f}}$, two new candidate chromosomes are generated by using the uniformly distributed random values μ_k by satisfying $\mu_k > 0$ and $\sum_{k=1}^{3} \mu_k = 1$. These are computed as

$$\mathbb{V}(\mathcal{G}+1)_{\check{m}} = \mu_1 \mathbb{V}(\mathcal{G})_{\check{m}} + \mu_2 \mathbb{V}(\mathcal{G})_{\check{f}} + \mu_3 \mathbb{V}(\mathcal{G})_{\check{b}}, \tag{24}$$

$$\mathbb{V}(\mathcal{G}+1)_{\check{f}} = \mu_2 \mathbb{V}(\mathcal{G})_{\check{m}} + \mu_1 \mathbb{V}(\mathcal{G})_{\check{f}} + \mu_3 \mathbb{V}(\mathcal{G})_{\check{b}}. \tag{25}$$

The fundamental concept of the proposed approach lies in its crossover mechanism, which incorporates three components, i.e., two selected parents and the best-performing individual from previous generations, denoted by $\mathbb{V}(\mathcal{G})_{\check{b}}$, unlike conventional GA methods that rely on two parents. This structure supports a dual search strategy, i.e., local exploration around the parents and a directed greedy search toward the globally optimal candidate. Integrating this hybrid mechanism effectively merges CGA's population diversity with PSO's rapid convergence, ensuring offspring are steered toward optimal solutions. The hybrid CGA-PSO algorithm is as computationally efficient[4] as CGA, while also improving performance, especially in escaping local optima and rapid convergence. The mutation phase further enhances diversity by modifying chromosomes at a low mutation rate (R_m). This step is essential to prevent the population from becoming overly homogeneous across successive generations. It involves inserting Gaussian-distributed random variables with 0 mean and 0.05 standard deviation relative to the upper-bound entry length. The algorithm iteratively refines the population through successive selection, crossover, and mutation loops. Upon completion of the iterations, the optimized chromosome corresponding to the best solution is obtained as $\mathbb{V}^* = [\alpha^*, \beta^*, \epsilon^*, [\mathbf{q}_U^*]_{1\times 3}, P_S^*, P_D^*]$.

Next, we focus on addressing the constraints given in the optimization problem. Consequently, we modify the objective function by introducing penalty terms for constraint violations, as described in (22b)-(22f). The fitness value of an individual solution candidate is computed as

$$\begin{aligned}\text{Fitness}(\mathbb{V}_\Psi) = \mathcal{T}_{\text{sys}}^{\text{sec}} &- \Omega_1 \max(0, P_D - P_D^{\max}) \\ &- \Omega_2 \max(0, P_S - P_S^{\max}) - \Omega_3 \max(0, \mathcal{P}_{\text{sop}} - \gamma_s) \\ &- \Omega_4 \max(0, \alpha - 1) - \Omega_5 \max(0, \beta - 1) \\ &- \Omega_6 \max(0, \epsilon - 1) - \Omega_7 \max(0, \mathbf{q}_U - \mathbf{q}_U^{\max}) \\ &- \Omega_8 \max(0, \mathbf{q}_U^{\min} - \mathbf{q}_U),\end{aligned} \tag{26}$$

where $\Omega_i > 0\ \forall i \in \{1, 2, \ldots, 8\}$ ensure that penalty terms are properly enforced. The overall layout of the hybrid CGA-PSO algorithm-based secure framework is presented in Algorithm 1, providing an insightful overview for a glance at its key steps and operations.

[4]Despite the additional complexity introduced by incorporating $\mathbb{V}(\mathcal{G})_{\check{b}}$ in the crossover process, the computational burden remains minimal, requiring only a few extra multiplications [26].

Algorithm 1: Hybrid CGA-PSO Algorithm for SST Maximization

1) **Initialize:** Set population size ζ, crossover rate R_{co}, mutation rate R_m, maximum iterations τ^m, and initialize $\tau = 0$.
2) **Generate Initial Population:** Randomly generate chromosomes within the population $\mathbb{V}(0)_\psi, \forall \psi = 1, \ldots, \zeta$.
3) **Evaluate Fitness:** Compute the fitness of each chromosome $\mathbb{V}_\psi^{(\tau)}$ using (26).
4) **for** $\tau = 1$ to τ^m, **do:**
   a) **Selection:** Perform roulette-wheel selection based on fitness values to choose parents for reproduction.
   b) **Crossover:** Apply the hybrid CGA-PSO crossover mechanism:
      i) Select two parent chromosomes $\mathbb{V}(\mathcal{G})_{\check{m}}$ and $\mathbb{V}(\mathcal{G})_{\check{f}}$.
      ii) Incorporate best-performing individual from previous generations $\mathbb{V}(\mathcal{G})_{\check{b}}$.
      iii) Generate offspring using (24) and (25).
   c) **Mutation:** Introduce diversity by mutating offspring with probability R_m, using Gaussian-distributed noise with mean 0 and standard deviation 0.05 relative to the upper-bound entry length.
   d) **Constraint Handling:** Apply penalty functions for constraint violations as per (26).
   e) **Update Population:** Form the new population for the next generation.
5) **End for**
6) **Output:** Optimized solution $\mathbb{V}^* = [\alpha^*, \beta^*, \epsilon^*, [\mathbf{q}_U^*]_{1\times 3}, P_S^*, P_D^*]$.

2) Convergence Analysis: Now, we analyze the convergence behavior of the proposed hybrid algorithm by examining its key stages, i.e., selection, crossover, and mutation. According to the roulette selection, the probability of selecting an individual $\mathbb{V}_{\check{m}}$ for reproduction in $(\mathcal{G}+1)$th generation is proportional to its fitness $\mathcal{F}_{\check{m}}$ in $\mathcal{G}$, given as

$$\Pr_{(\mathcal{G}+1)}(\mathbb{V}_{\check{m}}) = \frac{\mathcal{F}_{\check{m}}}{\sum_{\check{f}} \mathcal{F}_{\check{f}}}. \tag{27}$$

Since an individual solution $\mathbb{V}_{\check{m}}$ may not be unique and can have duplicates in the population, $\Pr_{(\mathcal{G}+1)}(\mathbb{V}_{\check{m}})$ depends on the number of its occurrences, denoted as $K_{\check{m},\mathcal{G}}$, is given by

$$\Pr_{(\mathcal{G}+1)}(\mathcal{F}_{\check{m}}) = K_{\check{m},\mathcal{G}} \frac{\mathcal{F}_{\check{m}}}{\sum_{\check{f}} \mathcal{F}_{\check{f}}} = \Pr_{(\mathcal{G})}(\mathcal{F}_{\check{m}}) \frac{\mathcal{F}_{\check{m}}}{\overline{\mathcal{F}}_{\check{m}}}, \tag{28}$$

where $\overline{\mathcal{F}}_{\check{m}} = \frac{\sum_{\check{f}} \mathcal{F}_{\check{f}}}{K_{\check{m},\mathcal{G}}}$. This ensures that the probability of selecting a candidate solution in the next generation is proportional to its fitness and occurrences in the current generation.

This mechanism favors individuals with higher fitness, causing their probabilities to grow exponentially over generations while the likelihood of selecting low-fitness individuals diminishes. Assuming a uniform initial fitness distribution and a maximum fitness M, the average fitness in generation $\mathcal{G}$, denoted by $\bar{\mathcal{F}}_{\mathcal{G}}$, is given as

$$\bar{\mathcal{F}}_{\mathcal{G}} = \int_0^M b_{\mathcal{G}}\, \mathcal{F}^{\mathcal{G}+1}\, d\mathcal{F} = \frac{\mathcal{G}+1}{\mathcal{G}+2} M, \tag{29}$$

where $b_{\mathcal{G}}$ is a normalization factor, given as $b_{\mathcal{G}} = \frac{\mathcal{G}+1}{M^{\mathcal{G}+1}}$ [24]. This indicates that the average fitness approaches M at a rate of $M/(\mathcal{G}+2)$, demonstrating the convergence trend. In the crossover stage, variability is introduced by combining genetic material from selected parents. The offspring, computed in (24) and (25), includes $\mu_1, \mu_2, \mu_3 > 0$ with $\mu_1 + \mu_2 + \mu_3 = 1$. This triangular combination allows exploration within the convex hull formed by the three parents, enhancing the local search capability and promoting diversity. Lastly, the mutation stage introduces variability by adding Gaussian noise to selected individuals, ensuring exploration beyond the current search space. This step helps maintain genetic diversity and prevents premature convergence. Overall, the hybrid approach leverages the greedy and uphill nature of incorporating $\mathbb{V}_{\mathcal{G}}$ for local searches, improving the likelihood of generating high-fitness offspring. The mean fitness curve exhibits progressive improvement and occasional fluctuations due to mutation effects, leading to faster and more robust convergence.

3) Computational Complexity: The computational complexity of Algorithm 1 is primarily determined by the nested loops governing fitness evaluation, crossover and mutation operations, and selection. The fitness evaluation step incurs a complexity of $O(\zeta)$ per generation due to its dependence on a feed-forward loop. The crossover and mutation operations contribute an additional complexity of $O(P_{\text{co}}\zeta + P_m\zeta)$ per iteration, where P_{co} and P_m represent the probabilities of crossover and mutation, respectively. The roulette-wheel selection mechanism requires $O(\zeta)$ operations for forming the selection array and $O(\ln\zeta)$ operations for selecting individuals, leading to an overall complexity of $O(\zeta\ln\zeta)$ per generation. Summing these components over the maximum number of iterations $\mathcal{G}^m$, the total complexity is expressed as $O(\zeta\mathcal{G}^m) + O((P_{\text{co}}\zeta + P_m\zeta)\,\mathcal{G}^m) + O((\zeta\ln\zeta)\,\mathcal{G}^m)$. Since P_{co} and P_m are constants, they do not affect the asymptotic growth rate, making the dominant term $O(\zeta\ln\zeta)\,\mathcal{G}^m)$. This final complexity expression encapsulates the scalability of the algorithm with respect to population size ζ and the number of iterations $\mathcal{G}^m$.

V. Numerical Results

In this section, we provide numerical and simulation results for SOP and SST and verify the accuracy of the analytical formulations. Unless specified in the particular figures, various parameters used for the simulations are listed as follows. We consider the transmit SNR as P_T/N_0, the codeword and confidential data transmission rates are set to $\mathcal{R}_{\text{b}} = 2$ bps/Hz and $\mathcal{R}_{\text{c}} = 1$ bps/Hz, respectively and $\eta_1 = \eta_2 = 0.7$. The EH parameters are set as $\alpha = 0.4$, and $\beta = 0.3$, and PAF for information and jamming signal is taken as $\epsilon = 0.5$ [22]. The fading severity parameter $m_{ij} = 2$, and the LoS component power for U_R to terrestrial links is $\lambda_{Uk} = 1.5$, and that for the terrestrial links is $\lambda_{SE} = \lambda_{DE} = 1.2$ [35]. The 3D coordinates of S, D, and E are given by $\mathbf{w}_S = (0, 50, 0)$, $\mathbf{w}_D = (200, 50, 0)$, and $\mathbf{w}_E = (100, 50, 0)$, respectively. We set the U_R's coordinates as $\mathbf{q}_U = (100, 50, 100)$, Whereas, for optimizing the U_R's position, $\mathbf{q}_U^{\min} = (0, 0, 0)$ $\mathbf{q}_U^{\max} = (200, 100, 120)$. The PL exponents for the LoS and NLoS links between the nodes, i.e., $\alpha_{\text{LoS}} = 2$ and $\alpha_{\text{NLoS}} = 3.5$. The expressions of SOP, derived in (17) and (18), have infinite series that are truncated by taking 20 summation terms to achieve a fair accuracy in obtaining the final value. In addition, we use the non-central chi-squared distribution to obtain the Be-Xi distributed random variable [31]. The Monte-Carlo simulation is performed by averaging the channel coefficients for 10^5 iterations.

First, we demonstrate the effectiveness of the considered system, which employs a hybrid TS-PS-based SWIPT model and a destination-assisted cooperative jamming (TS-PS-DJ) technique for a UAV-assisted secure network. To evaluate the security performance of the proposed scheme, the following baseline techniques are used for comparison:

- TS-based SWIPT architecture with destination-assisted jamming technique (TS-DJ).
- PS-based SWIPT architecture with destination-assisted jamming technique (PS-DJ) [21].
- TS-PS-based SWIPT architecture without destination jamming technique (TS-PS-WDJ).
- TS-PS-based SWIPT architecture with source-assisted jamming technique (TS-PS-SJ). In this case, S simultaneously transmits the information and jamming signals with a PAF. This model can be obtained by replacing the $P_D L_{DU}|h_{DU}|^2$ term with $P_{AN} L_{SU}|h_{SU}|^2$ in (5)-(14) and following similar steps to obtain the security metrics.
- PS-based SWIPT architecture with source-assisted jamming technique (PS-SJ). This model can be obtained by putting $\alpha = 0$ in (8) and replacing the $P_D L_{DU}|h_{DU}|^2$ term with $P_{AN} L_{SU}|h_{SU}|^2$ in (5)-(14) and following similar steps to obtain the security metrics.

A. Secrecy Outage Probability (SOP)

Figs. 3, 4, 5, 6, 7, 8, and 9 illustrate good agreement between the simulated and analytical results obtained for the SOP values with respect to the system and channel parameters. Specifically, Fig. 3 compares the SOP performance of the considered system with that of baseline methods. Overall, the proposed TS-PS-DJ scheme demonstrates the lowest SOP across all SNR values. This indicates that the hybrid SWIPT model with destination-assisted jamming provides better secrecy performance than existing architectures. The comparison curves demonstrate the proposed model's superior performance, showing its effectiveness in surpassing the individual TS and PS-based architectures. A notable observation is that the cooperative destination jamming technique significantly improves SOP performance compared to systems without jamming. This is because cooperative jamming degrades the SINR

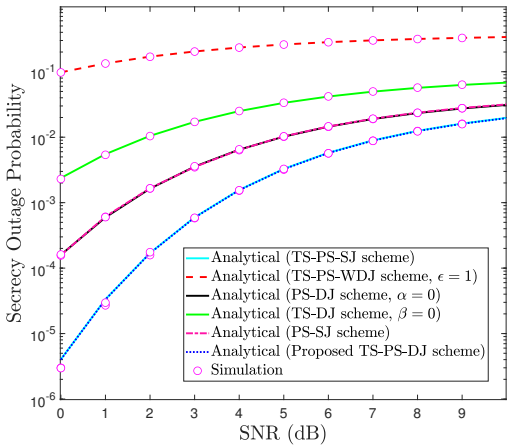

Fig. 3. Comparison of SOP with existing models.

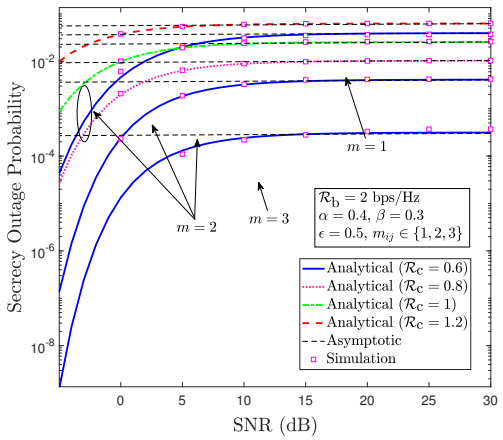

Fig. 4. SOP versus transmit SNR with varying $\mathcal{R}_c$.

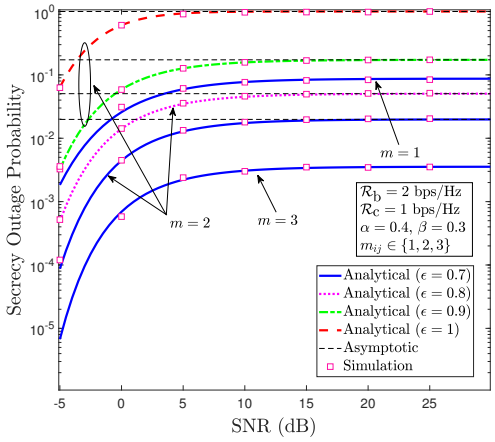

Fig. 5. SOP versus transmit SNR for different ϵ.

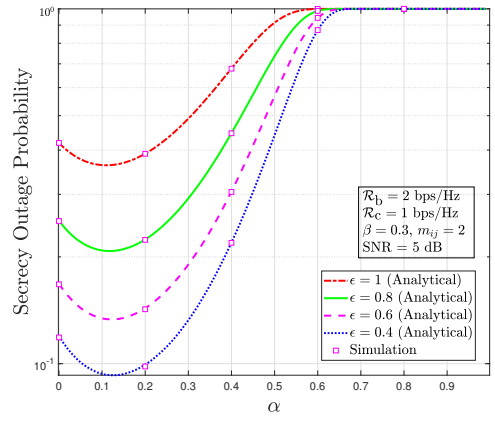

Fig. 6. SOP versus α for different ϵ.

at the eavesdropper, thereby reducing SOP and enhancing security. However, the PS-SJ and PS-DJ schemes exhibit similar SOP behavior, indicating that source-assisted and destination-assisted jamming provide comparable secrecy improvements. This confirms that jamming significantly enhances security, whether interfered from S or D. On the other hand, the TS-PS-WDJ scheme exhibits higher SOP than the jamming-based schemes since it lacks cooperative jamming, making it more vulnerable to eavesdropping. The individual TS-DJ and PS-DJ schemes perform better than TS-PS-WDJ but remain inferior to the proposed hybrid TS-PS-DJ scheme.

Figs. 4 and 5 show that both asymptotic and exact SOP curves perfectly match in the high SNR regime. It can be observed from these curves that after a specific SNR value, the SOP curves exhibit a saturated floor, beyond which a constant secrecy outage performance can be obtained even with the improvement of the eavesdropper's SINR. It can also be concluded that the SOP performance is improved with the increase in the values of $m_{ij} \in \{1, 2, 3\}$. This is due to the fact that the higher values of m_{ij} account for the lesser severe fading scenarios. In particular, Fig. 4 depicts the variation of the SOP with varying SNR for different values of $\mathcal{R}_c$ and m_{ij}. It is observed from the analysis that SOP increases with an increase in both transmit SNR and $\mathcal{R}_c$. This increment of SOP is due to a decrease in the rate difference, i.e., $\mathcal{R}_d = \mathcal{R}_b - \mathcal{R}_c$, which accounts for the cost of securing the information transmission against the E. However, the SOP curves become constant after 15 dB, which suggests that after this value, the instantaneous rate difference, $\mathcal{R}_b$ becomes equal to the instantaneous capacity at the E. The SOP value at which the saturation floor is obtained increases with the decrease in the $\mathcal{R}_c$ because of the fact that the lower $\mathcal{R}_c$ value corresponds to higher $\mathcal{R}_d$. Further, Fig. 5 shows the impact of ϵ on the SOP performance with the variation in transmit SNR. It can be observed from Fig. 5 that without destination jamming, the SOP value becomes very high and almost reaches 1 at 5 dB, which means the system's security is in the outage. It is noted that the system shows better SOP performance for the lower ϵ values, which is because P_D increases with the decrease in the ϵ value. Similar to Fig. 4, the SOP value attains the saturation even after decreasing ϵ and increasing transmit SNR. However, a further decrease in ϵ would affect the network's reliability as the allocated power for IT from S will be reduced.

The variation of SOP with respect to α for different ϵ values is depicted in Fig. 6. From the plot, we can infer

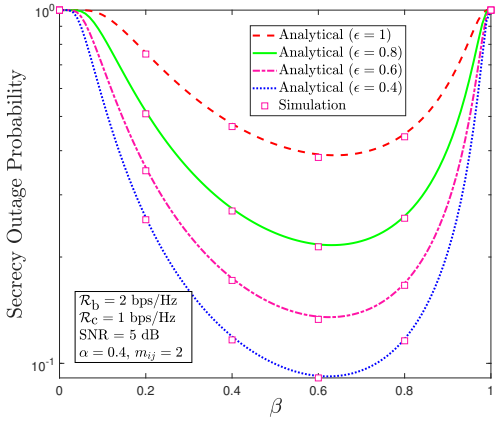

Fig. 7. SOP versus β for different ϵ.

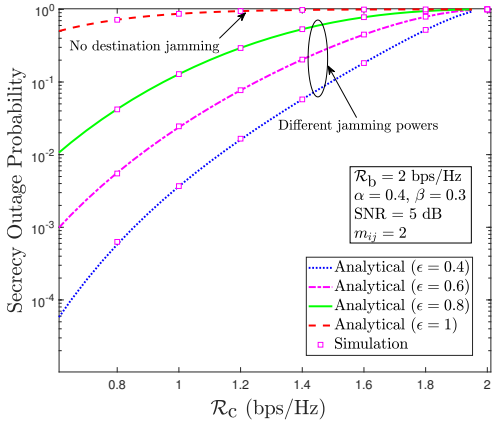

Fig. 8. SOP versus $\mathcal{R}_c$ for different ϵ.

that the SOP is minimum for the lower values of α, which slightly increases with the increasing ϵ values from $0.4 - 1$ and drastically increases for $\alpha > 0.2$. It is evident from the plot that lower α values correspond to less time allocated to EH and more time allocated to IT, which results in better SOP performance. Moreover, Fig. 6 shows that the SOP approaches unity at lower α values for larger values of ϵ. The curves depict an optimal value of α for the ϵ values that can be obtained for minimizing the SOP values. An interesting trend can be observed from Fig. 7, which is plotted between the SOP and β at different ϵ values where SOP decreases initially as the value of β increases, and after a particular value of β, it starts increasing. With $\epsilon = 0.4$, it can be marked that the system shows the best SOP performance. On the other hand, when the ϵ is set to 1, the system shows the worst performance. From these trends, we can infer that the system provides better SOP performance with higher β values for higher values of ϵ, whereas when ϵ is comparatively smaller, β needs to be reduced. Followed by, Fig. 8 depicts the variation of SOP with respect to $\mathcal{R}_c$ for different values of ϵ. From here, it can be observed that the SOP, corresponding to higher $\mathcal{R}_c$, approaches unity slowly. This is attributed to the fact that, with the fixed $\mathcal{R}_b$, as $\mathcal{R}_c$ varies from 0.6 to 2, the difference

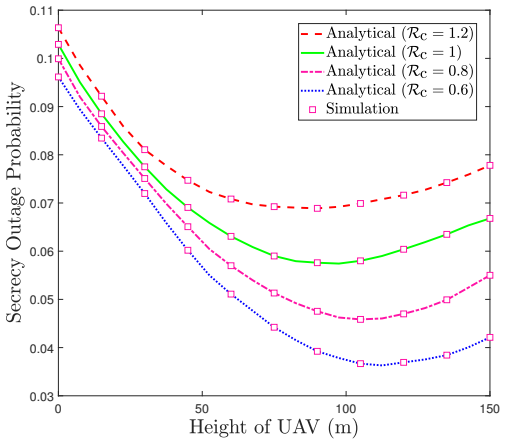

Fig. 9. SOP performance with respect to various UAV's height.

between $\mathcal{R}_b$ and $\mathcal{R}_c$ will be reduced to 0 and thus the secrecy of the information is compromised. It is also evident that with $\epsilon = 1$ (no cooperative jamming), the system reflects poor SOP performance compared to the lower ϵ values.

The variation of SOP with the UAV's height for different $\mathcal{R}_c$ values is shown in Fig. 9. We can observe that the curves exhibit unimodal convex behavior with respect to H. Specifically, as H increases, the SOP decreases rapidly to the minimum value and then rises again. This behavior can be attributed to better LOS conditions being obtained as H increases, which improves the A2G channels between U_R and terrestrial nodes. However, the PL of A2G links becomes more significant and affects the SOP performance with the further increase in H values, resulting in the SOP values increasing after attaining the minimum value. Fig. 9 also highlights that the minimum SOP values occur at different UAV's optimal height. The results obtained using Algorithm 1 closely align with the analytical results.

B. System Secrecy Throughput (SST)

Figs. 10, 11, and 12 show the SST (bps/Hz) versus the transmit SNR. Specifically, Fig. 10 highlights the impact of the confidential information transmission rate variations on the SST. It can also be observed that the SST value at which the saturation is attained reduces with the increase in $\mathcal{R}_c$ value. This is attributed to the fact that as the confidential information rate increases, this results in decreasing the $\mathcal{R}_d$ (i.e., $\mathcal{R}_d = \mathcal{R}_b - \mathcal{R}_c$), thus increasing the saturation value of SOP and decreasing the system throughput. A similar trend can be observed in Fig. 11 that illustrates the impact of ϵ on the SST at different transmit SNR values. As explained in Section V-A, with the decrease in ϵ, the power corresponding to the information transmission reduces while the jamming power increases, thus improving the SOP performance. Since the SST depends on SOP, the throughput corresponding to lower ϵ shows improved performance compared to higher ϵ values in the low SNR region. Whereas the SST decreases up to the mid-SNR regime, it saturates to a fixed value corresponding to different ϵ.

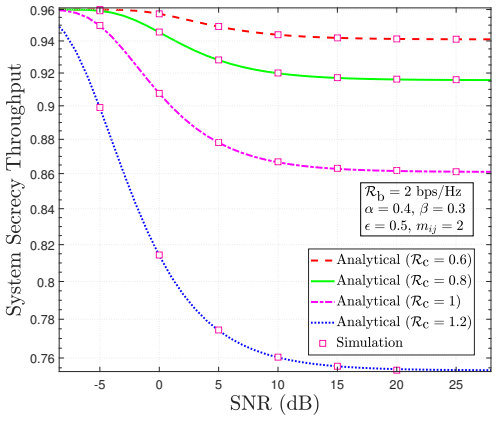

Fig. 10. SST versus transmit SNR for different $\mathcal{R}_c$.

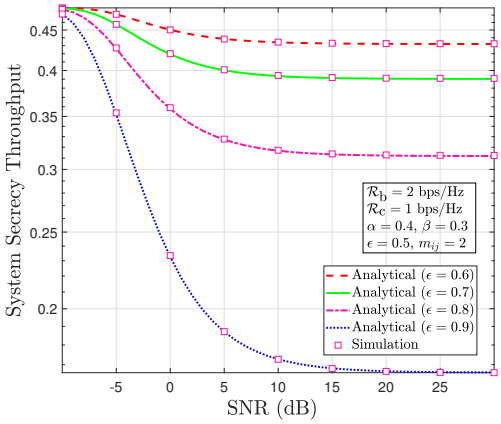

Fig. 11. SST versus transmit SNR for different ϵ.

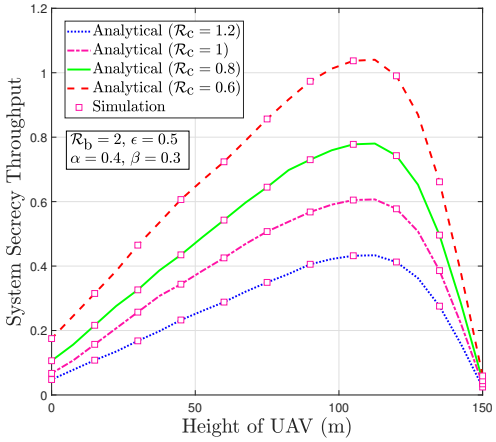

Fig. 12. SST performance with respect to various UAV's height.

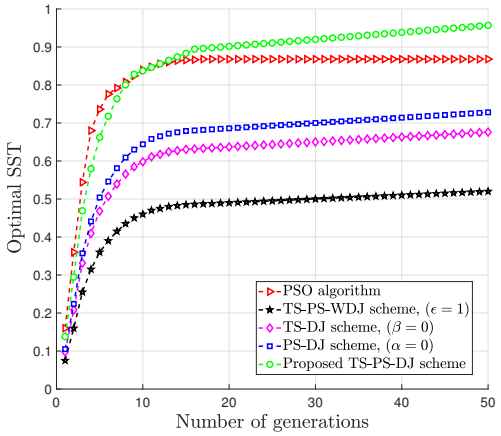

Fig. 13. Convergence curves for the proposed and baseline algorithms.

By observing the trends in Fig. 11, an important conclusion can be given that the secrecy throughput at $\epsilon = 1$ degrades at a higher rate. This is because the jamming power at $\epsilon = 1$ is 0, demonstrating the worst case for the system having no cooperative jamming. The variation of SST with the UAV's height for different $\mathcal{R}_c$ values is shown in Fig. 12. Specifically, as H increases, the SST increases to a maximum value before declining rapidly. This behavior can be clearly understood from the perspectives of the SOP curves in Fig. 9. The curves in Fig. 12 illustrate that there is an optimal U_R height, denoted as $\mathbf{H}^*$, that maximizes the SST. The results obtained using Algorithm 1 closely align with the analytical results, and it is noticed that the $\mathbf{H}^*$ lies between 112 m and 120 m.

C. Results With Optimized System Parameters

This section presents a comparative analysis of the proposed algorithm against baseline methods and existing algorithms from the literature. Herein, we compare the performance of the proposed TS-PS-DJ scheme, which is solved using the hybrid PSO-CGA method, to the baseline methods discussed in Section V. The convergence of the proposed and baseline algorithms over 50 generations is shown in Fig. 13, with performance summarized in Table II. The comparison highlights the superiority of the TS-PS-DJ scheme using the PSO-CGA hybrid algorithm, considering factors like generations to achieve 95% convergence, real runtime, and optimal SST values. The convergence curves in Fig. 13 illustrate that the proposed scheme, optimized using the PSO algorithm, achieves the fastest convergence, requiring only 11 generations to reach 95% convergence. However, this rapid convergence comes at the cost of suboptimal results, yielding an optimal SST of 0.868. In contrast, the proposed scheme utilizing the PSO-CGA-based hybrid algorithm attains a superior SST value of 0.98 despite requiring 17 generations for convergence. Among the baseline methods, the TS-PS-WDJ scheme converges in 14 generations, achieving an SST of 0.728. At the same time, the TS-DJ and PS-DJ schemes also require 14 generations but attain lower SST values of 0.676 and 0.52, respectively. These results highlight the effectiveness of the proposed PSO-CGA-based hybrid algorithm in achieving a better trade-off between convergence speed and optimal SST performance.

While the number of generations provides insight into convergence speed, actual runtime is equally significant due to the varying computational demands of different methods. The PSO

TABLE II
COMPARISON OF PROPOSED AND BASELINE ALGORITHMS

Baseline schemes	Number of Generations (95% convergence)	Run time (sec)	Optimal SST
TS-DJ scheme	14	1.6921	0.676
PS-DJ scheme	14	1.4928	0.520
TS-PS-WDJ scheme	14	1.7854	0.728
PSO algorithm	11	1.1834	0.868
Proposed scheme	17	1.7818	0.980

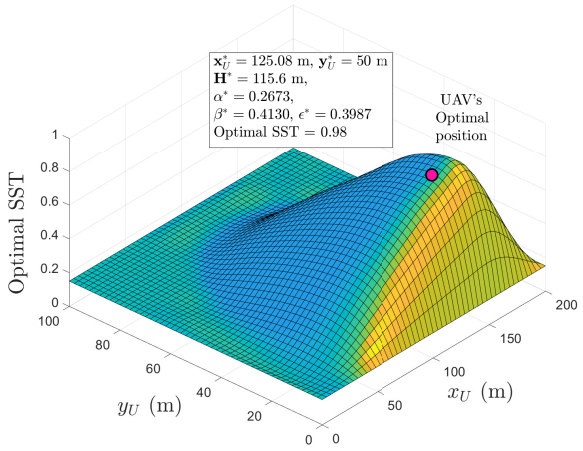

Fig. 14. UAV's 2D position with optimal SST.

algorithm achieves the lowest runtime of 1.183 seconds but at the cost of suboptimal SST performance, making it less competitive. Among the baseline schemes, PS-DJ exhibits better efficiency with a runtime of 1.492 seconds, outperforming TS-DJ, which requires 1.692 seconds. However, both schemes fall short in final SST performance compared to the proposed TS-PS-DJ scheme, highlighting the benefits of integrating time-switching and power-splitting with destination jamming. It can be observed that the proposed TS-PS-DJ scheme outperforms all baseline methods, achieving the highest optimal SST. With a runtime of 1.7958 seconds, it remains competitive while ensuring superior convergence characteristics and enhanced security performance, confirming its effectiveness in balancing optimization efficiency and computational cost.

The 3D surface plot in Fig. 14 illustrates the optimization results obtained using the proposed Algorithm 1. It presents the optimal positioning of the UAV relay (U_R) in terms of $\mathbf{x}_U$ and $\mathbf{y}_U$ coordinates to achieve the optimal SST value. Since S and D are fixed on the ground, the UAV relay's ability to position itself strategically ensures efficient communication between S and D while enhancing security. By utilizing the proposed Algorithm 1, the optimal UAV position is determined as $\mathbf{x}_U^* = 125.08$ m, $\mathbf{y}_U^* = 50$ m, $\mathbf{H}^* = 115.6$ m, yielding an optimal SST of 0.98, as indicated by the red-highlighted point in Fig. 14. These values validate the efficiency of the optimization approach in selecting an optimal UAV position that maximizes security performance. Furthermore, the improvement in SST performance is achieved by optimizing key system parameters, namely, $\alpha^* = 0.2673$, $\beta^* = 0.4130$, and $\epsilon^* = 0.3987$, which are obtained through the proposed optimization framework.

VI. CONCLUSION

This paper has considered an energy-constrained UAV-mounted AF-based relay that assists information transmission between the source and destination where the LoS path is heavily obstructed. In this scenario, there is a terrestrial eavesdropper in the vicinity of the source and destination who can wiretap the information by exploiting A2G channels. Thus, we have employed a hybrid TS-PS-based SWIPT technique at the UAV relay to enhance the network lifetime and destination-aided cooperative jamming to strengthen security. For this setup, we have derived closed-form expressions for the SOP and SST over Be-Xi distributed channels to assess performance with various channel parameters. Moreover, we have performed the asymptotic SOP in a high SNR regime to obtain critical insights into the system's performance. The accurate expression of SST is utilized as an objective function for formulating the SST maximization problem by jointly optimizing the system parameters such as transmit powers of S and D, power allocation factor, SWIPT parameters, and UAV 3D location. The formulated problem has complex and non-convex objective functions with tightly coupled optimizing variables. Therefore, we employed a hybrid CGA-PSO algorithm to solve the complex multi-variable problem efficiently. Lastly, we have demonstrated that our proposed TS-PS-based SWIPT scheme solved using the hybrid CGA-PSO algorithm significantly improved the system's throughput as compared to the baseline methods.

APPENDIX A
PROOF OF LEMMA 1

To obtain the expression of $\mathcal{P}_1$, we substitute the value of γ_{SE} obtained in (10) into (16) as

$$\begin{aligned}\mathcal{P}_1 &= \Pr[\gamma_{SE} \le \delta_d] = \Pr\left[\frac{P_S L_{SE}|h_{SE}|^2}{P_D L_{DE}|h_{DE}|^2 + N_0} \le \delta_d\right] \\ &= \Pr\left[|h_{SE}|^2 \le A|h_{DE}|^2 + B\right]. \end{aligned} \tag{30}$$

Let $A = \frac{P_D L_{DE}\delta_d}{P_S L_{SE}}$ and $B = \frac{N_0\delta_d}{P_S L_{SE}}$, $X \triangleq |h_{SE}|^2$ and $Y \triangleq |h_{DE}|^2$, where X and Y are Be-Xi distributed random variables. Using the expectation property of bi-variate random variables, (30) can be expressed in an integral form as

$$\mathcal{P}_1 = \int_0^\infty F_X(Ay + B) f_Y(y) dy. \tag{31}$$

The CDFs and PDFs of Be-Xi distributed random variables X and Y can be obtained by using the transformation of RV which are given as

$$F_X(x) = 1 - Q_m\left(\sqrt{\frac{2m}{\Omega}}\lambda, \sqrt{\frac{2m}{\Omega}x}\right), \tag{32}$$

$$f_X(x) = \frac{1}{2}\left(\frac{2me^{-\frac{m}{\Omega}(\lambda^2+x)}}{\Omega\lambda^{m-1}}\right) x^{\frac{(m-1)}{2}} \mathcal{I}_{m-1}\left(\frac{2m\lambda}{\Omega}\sqrt{x}\right). \tag{33}$$

By using (32), we can get the CDF term required for (31)

$$F_X(Ay+B) = 1 - \sum_{\rho=0}^{\infty} \sum_{k=0}^{\rho+m_{SE}-1} \sum_{s=0}^{k} \binom{k}{s} \left(\frac{m_{SE}}{\Omega_{se}}\right)^{\rho+k} \times \frac{A^s B^{k-s} y^s \lambda_{SE}^{2\rho}}{\rho!\ k!} e^{-\left(\frac{m_{SE}}{\Omega_{SE}}(\lambda_{SE}^2 + Ay + B)\right)}. \quad (34)$$

For deriving the closed form expression and for the accurate truncation of the results, we accurately employ the approximated Bessel function as [41]

$$\mathcal{I}_v(x) = \sum_{r=0}^{q} \mathbb{F}[q, r, v]\, (x/2)^{v+2r}, \quad (35)$$

where $\mathbb{F}[q,r,v] = \frac{\Gamma(q+r)q^{(1-2r)}}{\Gamma(r+1)\Gamma(q-r+1)\Gamma(v+r+1)}$. It is observed that as the $q \sim \infty$, (35) results in terms of the infinite series [35]. By using (33) and (35), the PDF expression can be given as

$$f_Y(y) = \sum_{c=0}^{C} \frac{\lambda_{DE}^{2c}\ \Gamma(C+c)\ (C)^{1-2c}}{\Gamma(c+1)\ \Gamma(C-c+1)\ \Gamma(c+m_{DE})} \times \left(\frac{m_{DE}}{\Omega_{DE}}\right)^{m_{DE}+2c} y^{m_{DE}+c-1} e^{-\left(\frac{m_{DE}}{\Omega_{DE}}(\lambda_{DE}^2 + y)\right)}. \quad (36)$$

Substituting the (34) and (36) into (31) and after rearranging them, we obtain

$$\mathcal{P}_1 = 1 - \sum_{l=0}^{\infty} \sum_{k=0}^{l+m_{SE}-1} \sum_{c=0}^{C} \sum_{s=0}^{k} \binom{k}{s} \left(\frac{m_{SE}}{\Omega_{SE}}\right)^{l+k} \times \left(\frac{m_{DE}}{\Omega_{DE}}\right)^{m_{DE}+2c} e^{-\left(\frac{m_{SE}}{\Omega_{SE}}(\lambda_{SE}^2+B)\right)} e^{-\left(\frac{m_{DE}}{\Omega_{DE}}(\lambda_{DE}^2)\right)} \times \frac{A^s B^{k-s} \lambda^{2i} \lambda_{DE}^{2c}\ \Gamma(C+c)\ (C)^{1-2c}}{l!\ k!\ \Gamma(c+1)\ \Gamma(C-c+1)\ \Gamma(c+m_{DE})} \times \int_0^{\infty} y^{m_{DE}+s+d-1} e^{-\left(\frac{m_{SE}}{\Omega_{SE}}A + \frac{m_{DE}}{\Omega_{DE}}\right)y} dy. \quad (37)$$

Finally, we apply [42, eq. 3.381.4], the obtained closed form expression of $\mathcal{P}_1$ can be given in (17).

Appendix B
Proof of Lemma 2

To obtain the expression of $\mathcal{P}_2$, we substitute the value of γ_{UE} in (16), so $\mathcal{P}_2$ is obtained as

$$\mathcal{P}_2 = \Pr\left[\gamma_{UE} \le \delta_d\right] = \Pr\left[|h_{SU}|^2 \le \frac{\delta_d P_D L_{DU} |h_{DU}|^2}{P_S L_{SU}} + \frac{\delta_d N_0}{\varpi P_S L_{SU} L_{UE} |h_{UE}|^2} + \frac{\delta_d (2-\beta) N_0}{(1-\beta) P_S L_{SU}}\right]. \quad (38)$$

Let $U = |h_{SU}|^2$, $V = |h_{DU}|^2$ and $W = |h_{UE}|^2$, where U, V and W are Be-Xi distributed random variables with the CDF and PDF given in (32) and (33), respectively. On assuming $a_1 = \frac{\delta_d P_D L_{DU}}{P_S L_{SU}}$, $a_2 = \frac{\delta_d N_0}{\varpi P_S L_{SU} L_{UE}}$ and $a_3 = \frac{\delta_d (2-\beta) N_0}{(1-\beta) P_S L_{SU}}$, and substituting these variables in (38) and using the expectation operator, we obtain

$$\mathcal{P}_2 = \int_0^{\infty} \int_0^{\infty} F_U(a_1 v + \frac{a_2}{w} + a_3) f_V(v) f_W(w) dv dw. \quad (39)$$

Now, expanding $F_U(a_1 v + \frac{a_2}{w} + a_3)$ by using (32) and separating the integrals, we have

$$\mathcal{P}_2 = 1 - \int_0^{\infty} \int_0^{\infty} Q_m\left(\sqrt{\frac{2m}{\Omega}}\lambda, \sqrt{\frac{2m}{\Omega}(a_1 v + \frac{a_2}{w} + a_3)}\right) \times f_V(v) dv f_W(w) dw. \quad (40)$$

First, we substitute the value of Q-function followed by substituting the PDF of random variable V that follows Be-Xi distribution.

$$\mathcal{P}_2 = 1 - \int_0^{\infty} \Bigg\{ \sum_{r=0}^{\infty} \sum_{z=0}^{Z} \sum_{q=0}^{r+m_{SU}-1} \sum_{g=0}^{q} \binom{g}{q} \left(\frac{m_{DU}}{\Omega_{DU}}\right)^{m_{DU}+2z} \times \left(\frac{m_{SU}}{\Omega_{SU}}\right)^{q+r} \frac{a_1^{q-g} (\frac{a_2}{w} + a_3)^g \lambda_{SU}^{2r}\ \lambda_{DU}^{2z}}{r!\ q! \left(\frac{m_{SU}}{\Omega_{SU}} + a_1 \frac{m_{DU}}{\Omega_{DU}}\right)^{m_{DU}+l+q-g}} \times e^{-\left(\frac{m_{SU}}{\Omega_{SU}}(\lambda_{SU}^2 + \frac{a_2}{w} + a_3)\right)}\ e^{-\left(\frac{m_{DU}}{\Omega_{DU}}\lambda_{DU}^2\right)} \times \frac{\Gamma(Z+z)(Z)^{1-2z}\Gamma(m_{DU}+z+q-g)}{\Gamma(z+1)\Gamma(Z-z+1)\Gamma(m_{DU}+z)} \Bigg\} \times \Bigg\{ \sum_{\theta=0}^{\phi} \frac{\lambda_{UE}^{2\theta}\ \Gamma(\phi+\theta)(\phi)^{1-2\theta}}{\Gamma(\theta+1)\Gamma(\phi-\theta+1)\Gamma(m_{UE}+\theta)} \times \left(\frac{m_{UE}}{\Omega_{UE}}\right)^{m_{UE}+2\theta} w^{m_{UE}+\theta-1} e^{-\left(\frac{m_{UE}}{\Omega_{UE}}(\lambda_{UE}^2 + w)\right)} \Bigg\} dw. \quad (41)$$

On rearranging (41) and applying the mathematical formulations [42, eq. 3.471.9], we obtain the final expression of $\mathcal{P}_2$ as shown in (18).

References

[1] W. Sun, Z. Li, J. Shi, Z. Bai, F. Wang, and T. Q. S. Quek, "MAHTD-DDPG-based multi-objective resource allocation for UAV-assisted wireless network," *IEEE J. Miniaturization for Air and Space Systems*, pp. 1–1, 2024.

[2] Y. Bai, H. Zhao, X. Zhang, Z. Chang, R. Jäntti, and K. Yang, "Toward autonomous multi-UAV wireless network: A survey of reinforcement learning-based approaches," *IEEE Commun. Surveys & Tuts.*, vol. 25, no. 4, pp. 3038–3067, 2023.

[3] Z. Xiao, L. Zhu, Y. Liu, P. Yi, R. Zhang, X.-G. Xia, and R. Schober, "A survey on millimeter-wave beamforming enabled UAV communications and networking," *IEEE Commun. Surveys & Tuts.*, vol. 24, no. 1, pp. 557–610, 2022.

[4] G. K. Pandey, D. S. Gurjar, S. Yadav, Y. Jiang, and C. Yuen, "UAV-assisted communications with RF energy harvesting: A comprehensive survey," *IEEE Commun. Surveys & Tuts.*, pp. 1–1, 2024.

[5] T. D. Ponnimbaduge Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," *IEEE Commun. Surveys & Tuts.*, vol. 20, no. 1, pp. 264–302, 2018.

[6] N. P. Le, L. C. Tran, X. Huang, E. Dutkiewicz, C. Ritz, S. L. Phung, A. Bouzerdoum, D. Franklin, and L. Hanzo, "Energy-harvesting aided unmanned aerial vehicles for reliable ground user localization and communications under lognormal-nakagami-m fading channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1632–1647, 2021.

[7] D.-T. Do, A.-T. Le, Y. Liu, and A. Jamalipour, "User grouping and energy harvesting in UAV-NOMA system with AF/DF relaying," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11 855–11 868, 2021.

[8] X. Li, S. Cheng, H. Ding, M. Pan, and N. Zhao, "When UAVs meet cognitive radio: Offloading traffic under uncertain spectrum environment via deep reinforcement learning," *IEEE Trans. Wir. Commun.*, vol. 22, no. 2, pp. 824–838, 2023.

[9] M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk, and Z. Jin, "UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions," *IEEE Trans. Intelligent Vehicles*, vol. 9, no. 4, pp. 4583–4605, 2024.

[10] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wir. Commun.*, vol. 26, no. 5, pp. 12–18, 2019.

[11] H. Lei, M. Yang, J. Jiang, K.-H. Park, and G. Pan, "Secure offloading in NOMA-aided aerial MEC systems based on deep reinforcement learning," *IEEE J. Miniaturization for Air and Space Systems*, pp. 1–1, 2024.

[12] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security threats and mitigation techniques in UAV communications: A comprehensive survey," *IEEE Access*, vol. 10, pp. 112 858–112 897, 2022.

[13] D. Diao, B. Wang, K. Cao, R. Dong, and T. Cheng, "Enhancing reliability and security of UAV-enabled NOMA communications with power allocation and aerial jamming," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8662–8674, 2022.

[14] Y. Li, R. Zhang, J. Zhang, and L. Yang, "Cooperative jamming via spectrum sharing for secure UAV communications," *IEEE Wireless Commun. Letts.*, vol. 9, no. 3, pp. 326–330, 2020.

[15] Z. Wang, J. Guo, Z. Chen, L. Yu, Y. Wang, and H. Rao, "Robust secure UAV relay-assisted cognitive communications with resource allocation and cooperative jamming," *J. Commun. Net.*, vol. 24, no. 2, pp. 139–153, 2022.

[16] W. Lu, Y. Ding, Y. Gao, S. Hu, Y. Wu, N. Zhao, and Y. Gong, "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," *IEEE Trans. Industrial Informatics*, vol. 18, no. 4, pp. 2704–2713, 2022.

[17] W. Tian, X. Ding, G. Liu, Y. Dai, and Z. Han, "A UAV-assisted secure communication system by jointly optimizing transmit power and trajectory in the internet of things," *IEEE Trans. Green Commun. and Networking*, vol. 7, no. 4, pp. 2025–2037, 2023.

[18] M. Tariq, A. Saadat, R. Ahmad, Z. Abaid, and J. J. P. C. Rodrigues, "Enhanced border surveillance through a hybrid swarm optimization algorithm," *IEEE Sensors Journal*, vol. 23, no. 22, pp. 28 172–28 181, 2023.

[19] X. Pang, M. Liu, N. Zhao, Y. Chen, Y. Li, and F. R. Yu, "Secrecy analysis of UAV-based mmwave relaying networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 4990–5002, 2021.

[20] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys & Tuts.*, vol. 21, no. 4, pp. 3417–3442, 2019.

[21] M. Tatar Mamaghani and Y. Hong, "On the performance of low-altitude UAV-enabled secure AF relaying with cooperative jamming and SWIPT," *IEEE Access*, vol. 7, pp. 153 060–153 073, 2019.

[22] W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. Kwan Ng, G. Zhang, J. Tang, and O. A. Dobre, "Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4476–4489, 2020.

[23] G. K. Pandey, D. S. Gurjar, S. Yadav, D. Krstic, and Y. Jiang, "Secrecy analysis and optimization of UAV-assisted IoT networks with RF-EH and imperfect hardware," *IEEE Internet of Things J.*, pp. 1–1, 2025.

[24] V.-H. Dang, L.-M.-D. Nguyen, V. N. Vo, H. Tran, T. D. Ho, C. So-In, and S. Sanguanpong, "Throughput optimization for NOMA energy harvesting cognitive radio with multi-UAV-assisted relaying under security constraints," *IEEE Trans. Cognitive Commun. and Networking*, vol. 9, no. 1, pp. 82–98, 2023.

[25] X. Gu, G. Zhang, M. Wang, W. Duan, M. Wen, and P.-H. Ho, "UAV-aided energy-efficient edge computing networks: Security offloading optimization," *IEEE Internet of Things J.*, vol. 9, no. 6, pp. 4245–4258, 2022.

[26] T. N. Nguyen, L.-T. Tu, P. Fazio, T. V. Chien, C. V. Le, H. T. T. Binh, and M. Voznak, "On the dilemma of reliability or security in unmanned aerial vehicle communications assisted by energy harvesting relaying," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 1, pp. 52–67, 2024.

[27] A. El Shafie, K. Tourki, and N. Al-Dhahir, "An artificial-noise-aided hybrid TS/PS scheme for OFDM-based SWIPT systems," *IEEE Commun. Letts.*, vol. 21, no. 3, pp. 632–635, 2017.

[28] G. Li, D. Mishra, Y. Hu, and S. Atapattu, "Optimal designs for relay-assisted NOMA networks with hybrid SWIPT scheme," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3588–3601, 2020.

[29] M. Oshaghi and M. J. Emadi, "Throughput maximization of a hybrid EH-SWIPT relay system under temperature constraints," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1792–1801, 2020.

[30] Y. Zhuang, X. Li, H. Ji, and H. Zhang, "Exploiting hybrid SWIPT in ambient backscatter communication-enabled relay networks: Optimize power allocation and time scheduling," *IEEE Internet of Things J.*, vol. 9, no. 24, pp. 24 655–24 668, 2022.

[31] N. C. Beaulieu and X. Jiandong, "A novel fading model for channels with multiple dominant specular components," *IEEE Wireess Commun. Letts.*, vol. 4, no. 1, pp. 54–57, 2015.

[32] X. Sun, W. Yang, and Y. Cai, "Secure communication in NOMA-assisted millimeter-wave SWIPT UAV networks," *IEEE Internet of Things J.*, vol. 7, no. 3, pp. 1884–1897, 2020.

[33] A. Olutayo, J. Cheng, and J. F. Holzman, "A new statistical channel model for emerging wireless communication systems," *IEEE Open J. Commun. Society*, vol. 1, pp. 916–926, 2020.

[34] B. Zhu, Z. Zeng, J. Cheng, and N. C. Beaulieu, "On the distribution function of the generalized beckmann random variable and its applications in communications," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2235–2250, 2018.

[35] O. S. Badarneh, M. K. Awad, S. Muhaidat, and F. S. Almehmadi, "Performance analysis of intelligent reflecting surface-aided decode-and-forward UAV communication systems," *IEEE Sys. J.*, pp. 1–12, 2022.

[36] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys & Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2019.

[37] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Letts.*, vol. 15, no. 3, pp. 302–304, 2011.

[38] J. Hu, J. Shi, S. Ma, and Z. Li, "Secrecy analysis for orthogonal time frequency space scheme based uplink LEO satellite communication," *IEEE Wireless Commun. Letts.*, vol. 10, no. 8, pp. 2162–2345, 2021.

[39] Z. Tie, J. Shi, Z. Li, S. Li, and W. Liang, "Security performance analysis for an OTFS-based joint unicast-multicast streaming system," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6764–6777, 2022.

[40] C. Wang, Z. Li, X.-G. Xia, J. Shi, J. Si, and Y. Zou, "Physical layer security enhancement using artificial noise in cellular vehicle-to-everything (C-V2X) networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15 253–15 268, 2020.

[41] L. L, F. Li, and F. Gross, "A new polynomial approximation for Jv bessel functions," *Applied Mathematics and Computation*, vol. 183, no. 2, pp. 1220–1225, 2006.

[42] A. P. Prudnikov, "Integrals, and series: More special functions," *vol. 3. New York, NY, USA: Gordon Breach Sci.*, 1990.