IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 26, 2019, accepted October 15, 2019, date of publication October 18, 2019, date of current version October 31, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2948384*

# On the Performance of Low-Altitude UAV-Enabled Secure AF Relaying With Cooperative Jamming and SWIPT

**MILAD TATAR MAMAGHANI AND YI HONG, (Senior Member, IEEE)**
Department of Electrical and Computer Systems Engineering, Monash University, Clayton, VIC 3800, Australia
Corresponding author: Milad Tatar Mamaghani (milad.tatarmamaghani@monash.edu)

This work was supported in part by the Australian Research Council under Project DP160100528.

**ABSTRACT** This paper proposes a novel cooperative secure unmanned aerial vehicle (UAV) aided transmission protocol, where a source sends confidential information to a destination via an energy-constrained UAV-mounted amplify-and-forward relay in the presence of a ground eavesdropper. We adopt destination-assisted cooperative jamming as well as simultaneous wireless information and power transfer at the UAV-mounted relay to enhance physical-layer security and transmission reliability. Assuming a low-altitude UAV, we derive connection probability, secrecy outage probability, instantaneous secrecy rate, and average secrecy rate of the proposed protocol over Air-Ground channels, which are modeled as Rician fading with elevation-angel dependent parameters. Further, we analyze the asymptotic average secrecy rate performance of the proposed UAV-relaying scheme and derive high signal-to-noise ratio measures of the average secrecy rate to highlight the effect of various channel features on the system performance. By simulations, we verify our novel theoretical exact and approximate results and demonstrate significant performance improvement of our protocol, when compared to conventional transmission protocol with ground relaying and UAV-based transmission protocol without exploiting destination jamming. Finally, we evaluate the impacts of various system parameters, specifically, find the optimal UAV placement on the proposed protocol in terms of the aforementioned secrecy metrics.

**INDEX TERMS** UAV-relaying, 5G networks, cooperative jamming, physical-layer security, SWIPT.

## I. INTRODUCTION

Unmanned aerial vehicle (UAV) based wireless communications has recently attracted significant research attentions from both academia and industry. As a matter of fact, owning to the prominent attributes of UAVs such as maneuverability, adaptive altitude adjustment with the capability of hovering in the air; e.g., rotary-wing UAVs, ease of deployment with low acquisition and maintenance costs, and so forth, this emerging paradigm of UAV applications is envisioned to play a paramount role in establishing and/or improving ubiquitous and seamless connectivity of communication devices as well as enhancing capacity of future wireless networks [1]–[6].

UAVs have been introduced as aerial relays (see [7]–[10] and references therein) in support of long-distance data transmissions from source to destination in heavily shadowed environments and/or highly overloaded scenarios. Typically, due to UAVs mobility, UAVs require a sufficiently high energy resources for the propulsion and communications purposes, which can be supported via various energy harvesting techniques from ambient resources such as solar energy [11], wireless energy harvesting (WEH) [12], as well as simultaneous wireless information and power transfer (SWIPT) [13]. WEH harvests energy in a controlled manner from the ambient radio-frequency (RF) signals, while SWIPT not only captures information signals, but also concurrently harvests energy of the same signals [13], [14]. Specifically, a power splitting (PS) architecture is required to divide the received signal into two separate streams of different power levels, one for signal processing and the other for simultaneous energy harvesting [15]. One technical challenge of UAV-assisted communications is to guarantee physical-layer (PHY) security. The unique characteristics of Air-Ground (AG) channels can provide good channel

The associate editor coordinating the review of this manuscript and approving it for publication was Jiankang Zhang.

condition for legitimate nodes, but, on the other hand, is prone to eavesdropping by non-legitimate nodes [16], [17].

### A. RELATED WORK AND MOTIVATION

Exploiting PHY-security techniques in UAV-assisted communications has been studied in [18]–[20] (see references therein). In [18], the authors have studied PHY-security of a UAV-enabled mobile relaying scheme over non-fading AG channels, and showed that moving buffer-aided relay provides significant performance over static relaying in terms of the secrecy rate. In [19], the authors studied the resource allocation and path-planning problem for energy-efficient secure transmission from a UAV base station to multiple users in the presence of a passive ground eavesdropper. In [20], employing UAV as a friendly jammer to enhance PHY-security of a ground relaying (GR) scheme; wherein a terrestrial node is employed to extend the coverage of end-to-end communication, has been studied. However, a simple free-space path loss (PL) model for AG links have been adopted in the majority of previous literature which might be regarded as an oversimplified assumption in some environments.

Moreover, a tremendous amount of research studies have been focusing on the PHY-security paradigm with SWIPT technology [21]–[24]. A large-scale cognitive cellular network with wireless-powered device-to-device (D2D) framework has been introduced in [21] wherein the secrecy metrics of the considered network have been well investigated. Mamaghani *et al.* proposed a D2D communications via an untrustworthy amplify-and-forward (AF) relaying with SWIPT in the presence of an external jammer. They demonstrated the effectiveness of the jamming transmission in the studied three-phase time-switching based untrusted relay communications protocol and derived the closed-form expressions for various secrecy criteria in order to evaluate the secure communication [22], [25]. The study of SWIPT for non-security based UAV-assisted relay networks [23] and security based UAV-relaying [24] have been conducted. Specifically, in [24], the authors have examined SWIPT-enabled secure transmission of millimeter wave (mmWave) for a UAV-based relay network, where the UAV feeds the energy-constrained IoT destination device in the presence of multiple ground eavesdroppers. To the best of the authors knowledge, the potential of SWIPT for enhancing the energy-efficiency via energy harvesting and PHY-security of the UAV-derived networks has still been less understood and deserves further investigation.

### B. CONTRIBUTIONS

In this paper, we consider a practical scenario where a low-altitude UAV-relaying is employed to assist communications between a source-destination pair. Based on the recent channel measurements in [26], [27], low-altitude UAV-assisted relay channels may also suffer from small-scale fading compared to the AG links for high-altitude platforms. Hence, in this work we assume that AG channel models are Rician fading with different parameters while incorporated with probabilistic PL attenuation. Then, we tackle the aforementioned security and energy limitation challenges and make the following contributions.

- We propose a secure and energy-efficient transmission protocol, where a source sends confidential information to a destination via an energy-constrained UAV-mounted AF relay in the presence of a passive eavesdropper. In the protocol, we adopt the destination-assisted cooperative jamming (CJ) and SWIPT techniques at the UAV-based relay for the PHY-security improvements as well as energy harvesting.
- We analyze the proposed secure transmission protocol in terms of reliability and security. In particular, we derive connection probability, secrecy outage probability, instantaneous secrecy rate, and average secrecy rate of the proposed protocol from source to destination via UAV-relaying.
- We conduct simulations to *i*) verify our theoretical results, *ii*) identify the best location of the UAV-based relay that provides the best average secrecy rate, *iii*) evaluate impacts of different system parameters on the system performance in terms of reliability and security, and finally *iv*) validate the effectiveness and improvements of the proposed protocol, when compared to conventional transmission protocol with GR scheme and UAV-based relaying (UR) without destination-assisted jamming.

The rest of this paper is organized as below. Section II presents system model and channel model. In Section III, we propose the UAV-based transmission protocol with destination-assisted jamming and SWIPT techniques. In Section IV, we conduct performance analysis. Numerical results are given in Section V, and finally, conclusions are drawn in Section VI.

## II. SYSTEM MODEL AND CHANNEL MODEL

In this section, we first introduce the system model and then the assumptions for the channel model are given.

### A. SYSTEM MODEL

We consider a point-to-point secure transmission scheme (see Fig. 1), where we employ a UAV-mounted relay ($\mathbb{U}$) to assist confidential transmission from a source node Alice, denoted by $\mathbb{A}$, to a legitimate destination node Bob, namely $\mathbb{B}$, over heavily shadowed areas in the presence of Eve; a ground passive eavesdropper indicated by $\mathbb{E}$. The source, destination, and eavesdropper nodes are fixed on the ground, and without loss of generality, have the 3D coordinates as: $W_A = (A_x, A_y, 0)$, $W_B = (B_x, B_y, 0)$, $W_E = (E_x, E_y, 0)$, respectively. Whereas, the UAV is hovering in the sky and located at $W_U = (U_x, U_y, H)$ where $H$ is its altitude from ground surface.

We assume that all the nodes equipped with a single antenna operating in a half-duplex mode and $\mathbb{U}$ adopts AF protocol. Further, we assume that $\mathbb{U}$ leverages the

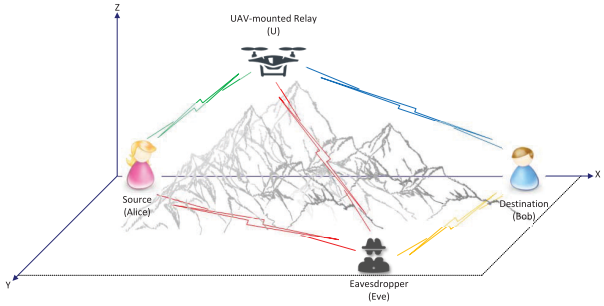


**FIGURE 1.** UAV-mounted low-altitude secure relaying communication based on destination-assisted jamming and SWIPT.

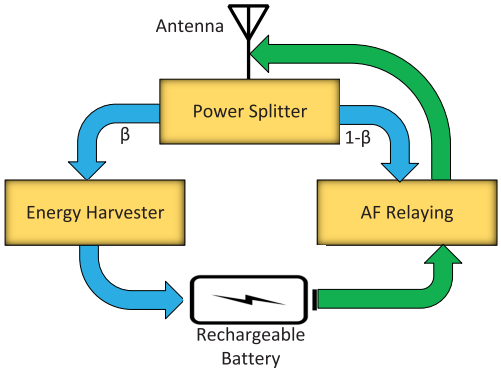


**FIGURE 2.** Power splitting structure for the SWIPT-enabled relaying at UAV.

SWIPT technology to harvest energy from the received RF signals transmitted by both $\mathbb{A}$ and $\mathbb{B}$, while it also utilises its on-board battery for maneuvering and staying stationary in the sky. Finally, we assume that the UAV receiver adopts power splitting architecture (see Fig. 2), where $\beta$ ($0 \leq \beta \leq 1$) is the power splitting ratio (PSR) identifying the fraction of the harvested power from the received RF signals and $(1-\beta)$ denotes the portion of which is dedicated for signal processing at the AF UAV-relay.

### B. CHANNEL MODEL

Here we consider both *small-scale fading* and *large-scale PL* in setting up the channel model. We assume the channel between $\mathbb{U}$ and the ground node $\mathbb{G} \in \{\mathbb{A}, \mathbb{B}, \mathbb{E}\}$ is *Rician fading* but with different values of Rice parameters. Exploiting channel reciprocity, the normalized channel power gain between the links $\mathbb{A} \Leftrightarrow \mathbb{U}$, $\mathbb{U} \Leftrightarrow \mathbb{B}$, and $\mathbb{U} \Leftrightarrow \mathbb{E}$ denoted by

$$S_{ij} \triangleq |h_{ij}|^2, \quad \text{for} \quad ij \in \{au, ub, ue\} \tag{1}$$

follow a square Rice distribution (i.e., non-central chi-square (nc-$\chi^2$) distribution) with two degrees of freedom, corresponding to line-of-sight (LOS) and non-line-of-sight (NLOS) components whose probability density function (PDF) and cumulative distribution function (CDF) are

$$f_{ij}(x) = (K_{ij}+1)e^{-K_{ij}} \exp\Big(-(K_{ij}+1)x\Big) \times \mathrm{I}_0\Big(2\sqrt{K_{ij}(K_{ij}+1)x}\Big), \tag{2}$$

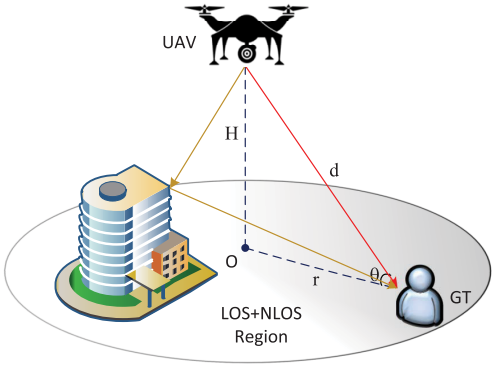


**FIGURE 3.** Illustration of considered elevation-angle-dependent low-altitude UAV channel model considering both LOS and NLOS links.

and

$$F_{ij}(x) = 1 - \mathrm{Q}\Big(\sqrt{2K_{ij}}, \sqrt{2(1+K_{ij})x}\Big), \tag{3}$$

where $x$ holds any non-negative value, $f_{ij}(\cdot)$ and $F_{ij}(\cdot)$ denote the PDF and the CDF for the link, and $\mathrm{I}_0(\cdot)$ represents the zeroth-order modified Bessel function of the first kind, $K_{ij}$ (in dB) is the *K-factor* given by

$$K_{ij}(\theta_{ij}) = \kappa_m + (\kappa_M - \kappa_m)\frac{2\theta_{ij}}{\pi}, \tag{4}$$

where $\theta_{ij}$ (in radian) is the elevation angle between two given nodes. For example as illustrated in Fig. 3 the elevation angle, denoted by $\theta$, between UAV with 3D position $W_U \in \mathbb{R}^{1\times 3}$ and ground terminal (GT) located at $W_G \in \mathbb{R}^{1\times 3}$, is given by $\theta \triangleq \mathbf{sin}^{-1}\frac{H}{\|W_U - W_G\|}$. Besides that, $\kappa_m$ and $\kappa_M$ (in dB) are two constants depending on the environment and transmission frequency. A point worth mentioning here is that (4), in some sense, illustrates the severity of fading of the environment as an exponential function of the elevation angle and these two constant parameters; i.e., $\kappa_m$ and $\kappa_M$, can be viewed as the minimum and maximum Rician factor occurring when $\theta_{ij} \to 0$ and $\theta_{ij} \to \frac{\pi}{2}$, respectively. Further, it should be mentioned that the general form of *K-factor* is obtained via on-site measurements in practice, however, in consistency with [28], the logarithmic expression given in (4) for the explicit relation between elevation angle and the shape parameter of Rician distribution for the sake of analysis. Furthermore, we assume the small-scale fading between any two GT nodes is Rayleigh fading [22], a special case of Rician fading when $K \to 0$, and thus the channel power gain for the GT links $\mathbb{A} \Leftrightarrow \mathbb{E}$, $S_{ae} \triangleq |h_{ae}|^2$, and $\mathbb{B} \Leftrightarrow \mathbb{E}$, $S_{be} \triangleq |h_{be}|^2$ can be modeled as exponential distribution with unit scale parameters.

Additionally, owning to the fact that for low-altitude UAVs the LOS path from UAV to terrestrial nodes may be blocked by various environmental obstacles, for the large scale channel attenuation we consider the probabilistic LOS model as in [28]–[30], adopting the elevation-angle

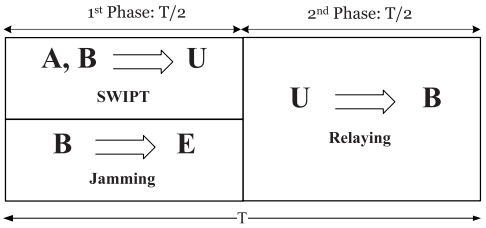


**FIGURE 4.** Diagram of the proposed secure UAV-relaying with SWIPT.

dependent PL component given by

$$\alpha_{ij}(\theta_{ij}) = \frac{\alpha_L - \alpha_N}{1 + \omega_1 \exp\left(-\omega_2\left(\theta_{ij} - \omega_1\right)\right)} + \alpha_N, \tag{5}$$

where $\alpha_L$ represents the PL exponent for the pure LOS link between two nodes which approximately corresponds to the condition when $\theta_{ij} \to \frac{\pi}{2}$, and also, when $\theta_{ij} \to 0$ the pure NLOS PL exponent, denoted by $\alpha_N$, is becoming the dominant component in (5) such that $\alpha_{ij}(0) \approx \alpha_N$. Further, $\omega_1$ and $\omega_2$ are some constants specified by the type of environment of interest; e.g., urban, rural, suburban, dense urban, and so forth. Letting $d_{ij} \triangleq \|W_i - W_j\|$ be the Euclidean distance between any two nodes either aerial or terrestrial one, $L_{ij}(\alpha_{ij}, d_{ij}) \triangleq d_{ij}^{-\alpha_{ij}}$ represents the large-scale attenuation when a signal transmitted by the node $i$ reaches the receiver of the node $j$ travelling through the wireless medium between. Note that for the terrestrial links with $\theta_{ij} \to 0$, the received signals have approximately undergone the pure NLOS propagation with the PL component $\alpha_N$, which is almost justifiable for the heavily shadowed fading environments, however, for the AG links the PL component is between $\alpha_L$ and $\alpha_N$ as a function of the elevation-angle between the aerial and GT nodes (see Fig. 3). Note that, it tends to be $\alpha_L$ when $\theta_{ij} \to \frac{\pi}{2}$. Hence, the adopted PL model, capturing both the distance and elevation angle features, is quite generic and satisfies both the AG and GT propagation characteristics.

## III. PROPOSED TRANSMISSION PROTOCOL

We consider the following two equal-duration phases of the proposed secure transmission protocol with an overall duration $T$ seconds (Fig. 4). During the first time slot, $\mathbb{A}$ sends information signal to $\mathbb{U}$ and simultaneously, $\mathbb{B}$ transmits a *jamming signal* to degrade the wiretap channel of $\mathbb{E}$ as well as to assist the energy harvesting operation of $\mathbb{U}$. Then the AF relay $\mathbb{U}$ receives

$$y_u = \sqrt{(1-\beta)P_a L_{au}} h_{au} x_a + \sqrt{(1-\beta)P_b L_{bu}} h_{bu} x_b + \sqrt{(1-\beta)} n_u + n_p, \tag{6}$$

where $x_a$ and $x_b$ denote the normalized information signal from $\mathbb{A}$, and jamming signal from $\mathbb{B}$, i.e.,

$$\mathbb{E}\{\|x_a\|^2\} = \mathbb{E}\{\|x_b\|^2\} = 1,$$

and $P_a$ and $P_b$ represent transmit power from $\mathbb{A}$ and jamming power from $\mathbb{B}$, which satisfy the total transmit power constraint as

$$P_a + P_b = P, \tag{7}$$

and $P$ is fixed for each frame. Further, we assume

$$P_a = \lambda P \quad P_b = (1-\lambda)P, \tag{8}$$

where $0 < \lambda < 1$ is the power allocation factor. Besides, $n_p$ represents signal processing noise at the power splitting component with power $N_p$, and $n_u$ representing the channel impairment due to thermal noise which is modeled as the Additive white Gaussian noise (AWGN) at $\mathbb{U}$; i.e., $n_u \sim \mathcal{N}(0, N_0)$ where $\mathcal{N}(\mu, \sigma^2)$ indicates the normal distribution with mean $\mu$ and variance $\sigma^2$.

The energy harvested by $\mathbb{U}$ from the received signals can be written as

$$E_H = \varepsilon\beta(P_a L_{au} S_{au} + P_b L_{bu} S_{bu} + N_0)\frac{T}{2}, \tag{9}$$

where $\varepsilon$ is the power conversion efficiency factor for the harvester. Here, we assume that the total harvested energy during the first phase will be used for signal transmission in the second phase and is given by

$$P_u = \varepsilon\beta(P_a L_{au} S_{au} + P_b L_{bu} S_{bu} + N_0). \tag{10}$$

Different from [18] where ignored the existence of direct link from $\mathbb{A}$ to $\mathbb{E}$, here we consider a more general scenario during which the malicious node $\mathbb{E}$ may take the advantage of information leakage in both the phases of communication due to broadcast nature of wireless media and then try to capture the confidential information. Specifically, if $\mathbb{E}$ is located on the ground that is not so far from $\mathbb{A}$, $\mathbb{E}$ can attempt to decode the received signal information during the first phase of transmission based on the received signal-to-interference-plus-noise ratio (SINR) as

$$\gamma_E^{(1)} = \frac{P_a L_{ae} S_{ae}}{P_b L_{be} S_{be} + N_0}. \tag{11}$$

In the second phase, $\mathbb{U}$ forwards the scaled version of $x_u = G y_u$ to $\mathbb{B}$ with the amplification factor

$$G = \sqrt{\frac{P_u}{(1-\beta)(P_a L_{au} S_{au} + P_b L_{bu} S_{bu} + N_0) + N_p}}, \tag{12}$$

where $P_u$ is in (10). The resultant signal at the node $\mathbb{K} \in \{\mathbb{E}, \mathbb{B}\}$ can be expressed as

$$\begin{aligned} \tilde{y}_k = & \underbrace{G\sqrt{(1-\beta)P_a L_{au} L_{uk}} h_{au} h_{uk} x_a}_{\text{Information signal component}} \\ & + \underbrace{G\sqrt{(1-\beta)P_b L_{bu} L_{uk}} h_{bu} h_{uk} x_b}_{\text{Destination jamming interference}} \\ & + \underbrace{G(\sqrt{(1-\beta)} n_u + n_p)\sqrt{L_{uk}} h_{uk} + n_k}_{\text{Noise}}, \end{aligned} \tag{13}$$

where $n_k \sim \mathcal{N}(0, N_0)$. Owning to the fact that $\mathbb{B}$ is assumed to be able to conduct full self-interference cancellation with regard to its own priori known jamming signal as in;

e.g., [22] and [31], hence the term of jamming interference can be subtracted from (13), whereas $\mathbb{E}$ acts with this part as an additional interference. Therefore, the received SINR at $\mathbb{B}$ and $\mathbb{E}$ can be obtained as

$$\gamma_{A\mapsto B} = \frac{\varepsilon\beta(1-\beta)P_a S_{au} S_{ub} L_{au} L_{ub}}{\varepsilon\beta(1-\beta+\zeta)S_{ub}L_{ub}N_0 + (1-\beta)N_0 + \epsilon}, \quad (14)$$

and

$$\gamma_E^{(2)} = \frac{\varepsilon\beta(1-\beta)P_a S_{au} S_{ue} L_{au} L_{ue}}{\varepsilon\beta(1-\beta)P_b S_{bu} S_{ue} L_{bu} L_{ue} + (1-\beta)N_0 + \varepsilon\beta\,(1-\beta+\zeta)\,S_{ue}L_{ue}N_0 + \epsilon}, \quad (15)$$

where

$$\zeta \triangleq \frac{N_p}{N_0} \quad \epsilon \triangleq \frac{N_p N_0}{P_a L_{au} S_{au} + P_b L_{ub} S_{ub}}. \quad (16)$$

Having considered that the information leakage is done in both first and second phases of transmission, a worst-case scenario is of our interest, wherein passive $\mathbb{E}$, performing the maximal ratio combining (MRC) of the received same signal for processing the intercepted confidential messages in two phases, poses a more detrimental attacks to the network. Toward this end, for the wiretap link, the resultant SINR at $\mathbb{E}$, denoted by $\gamma_E$, is given by

$$\gamma_E = \gamma_E^{(1)} + \gamma_E^{(2)}, \quad (17)$$

where $\gamma_E^{(1)}$ and $\gamma_E^{(2)}$ are given in (11) and (15), respectively.

## IV. PERFORMANCE ANALYSIS

In this section, we derive connection probability, secrecy outage probability, instantaneous secrecy rate, as well as achievable average secrecy rate of the proposed transmission protocol with high signal-to-noise ratio (SNR) analysis. In the derivations, we assume that the channel coefficients between nodes remain constants during each frame of communications and independently vary from one frame to next according to the block-fading assumption. Furthermore, for the rest of the paper, we assume $\epsilon = 0$ in (14) and (15) for simplicity of the results. This assumption holds for moderate/high SNRs.

### A. CONNECTION PROBABILITY

*Definition 1: The connection probability (CP), i.e., the probability that $\mathbb{B}$ is able to decode the transmitted signal from $\mathbb{A}$ and correctly extract the secure information messages [22], is defined as*

$$P_c \triangleq \Pr\{C_M > R_t\}, \quad (18)$$

*where*

$$C_M = \frac{1}{2}\log_2(1+\gamma_{A\mapsto B}), \quad (19)$$

*and $R_t$ denote the instantaneous capacity and transmission rate of $\mathbb{A}$-$\mathbb{B}$ via $\mathbb{U}$, which is normalized by bandwidth as [32], where $\gamma_{A\mapsto B}$ is given by (14).*

In order to optimize the connection probability with respect to (w.r.t) the parameters $(\lambda,\ \beta)$, we go a further step and formulate the following simple optimization problem

$$\begin{aligned} &\text{maximize } P_c(\lambda,\beta) \\ &\text{subject to } 0 \le \lambda, \beta \le 1 \end{aligned}$$

The objective function of the optimization problem given in (20) can be equivalently altered with the rational function $C_M(\lambda,\beta)$. Solving the above optimization problem yields to the optimal values as

$$\lambda^\star = 1, \quad \beta^\star = \frac{1}{1+\sqrt{\varepsilon\zeta S_{ub}L_{ub}}} \text{ for } \zeta > 1. \quad (20)$$

*Proof:* The proof is simple and hence ignored for brevity. ■

The following theorem provides an analytical closed-form expression of $P_c$.

*Theorem 1: We derive the CP of the secure UAV-based relaying in (21), as shown at the bottom of the next page, where $\delta_t \triangleq 2^{2R_t} - 1$, $D$ and $R$ are two positive integers controlling the accuracy of (21), $\Gamma(\cdot)$ represents the gamma function, $\zeta$ is given in (16), $d, u, s, r$ are dummy variables, $K_{ij}$, $ij \in \{au, ub\}$ is given in (4), and $\mathrm{I}_v(\cdot)$ is the modified Bessel function of the first kind with the order of $v$.*

*Proof: See Appendix A.* ■

*Remark:* From Theorem 1, we observe that (21) is a decreasing function w.r.t $P_a$, implying that as the source transmission power increases, the reliability of communication improves.

### B. SECRECY OUTAGE PROBABILITY

Following [33], when the instantaneous capacity of the wiretap link $C_E$, defined as

$$C_E = \frac{1}{2}\log_2(1+\gamma_E) \quad (22)$$

is larger than the rate difference $R_e = R_t - R_s$, where $R_s$ is the rate of the confidential information from $\mathbb{A}$-$\mathbb{B}$ via $\mathbb{U}$, then the secrecy outage occurs and the eavesdropper is able to intercept the transmitted confidential information via $\mathbb{U}$. The analytical expression for the secrecy outage probability (SOP), denoted by $P_{so}$, is given by Theorem below.

*Theorem 2: The analytical lower-bound closed-form expression for the SOP, $P_{so}$, is given as*

$$\begin{aligned} P_{so} &= \Pr\{C_E > R_e\} = \Pr\{\gamma_E > \delta_e\} \\ &\overset{(a)}{\ge} \Pr\{\max\left(\gamma_E^{(1)}, \gamma_E^{(2)}\right) > \delta_e\} \\ &= 1 - \underbrace{\Pr\{\gamma_E^{(1)} \le \delta_e\}}_{\mathcal{L}_1}\underbrace{\Pr\{\gamma_E^{(2)} \le \delta_e\}}_{\mathcal{L}_2}, \end{aligned} \quad (23)$$

*where $\delta_e \triangleq 2^{2R_e} - 1$ and $(a)$ follows from the inequality $\max\{x, y\} \le x + y$, and*

$$\mathcal{L}_1 = 1 - \frac{P_a L_{ae}\exp\left(-\frac{N_0\delta_e}{P_a L_{ae}}\right)}{P_b L_{be}\delta_e + P_a L_{ae}}, \quad (24)$$

*and $\mathcal{L}_2$ is given in* (25)*, as shown at the bottom of the this page, wherein $\mathrm{K}_\nu(\cdot)$ denotes the modified Bessel function with the second kind and $\nu$-th order and $d, u, r, q, s$ are dummy variables.*

*Proof: See Appendix B.* ∎

### C. INSTANTANEOUS SECRECY RATE

*Definition 2: The maximum achievable instantaneous secrecy rate (ISR), denoted by $C_S$, of the proposed UAV-enabled relaying network is defined as*

$$\begin{aligned} C_S &\triangleq [C_M - C_E]^+ \\ &= \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{A\mapsto B}}{1+\gamma_E}\right)\right]^+ \\ &= \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{A\mapsto B}-\gamma_E}{1+\gamma_E}\right)\right]^+, \end{aligned} \tag{27}$$

*where $[x]^+ \triangleq \max(x, 0)$, $C_M$ is the capacity between $\mathbb{A}$-$\mathbb{B}$ given in (19), and $C_E$ is the capacity of the wiretap link given in (22), and $\gamma_{A\mapsto B}$ and $\gamma_E$ are given in* (14) *and* (17)*, respectively.*

Reminding that the channel coefficients between nodes remain constants during each frame and vary from one frame to next independently; therefore, all parameters in (27) are assumed to be known except the power allocation factor $\lambda$, thereby we form the following optimization problem

$$\begin{aligned} \underset{\lambda}{\text{maximize}}\ & C_S(\lambda) \\ \text{subject to}\ & P_a + P_b = P \\ & P_a = \lambda P \\ & P_b = (1-\lambda)P. \end{aligned}$$

Considering $C_S \geq 0$ is guaranteed under optimal power allocation, the above optimization problem is equivalent to finding the optimal power allocation factor, i.e.,

$$\lambda^\star = \arg\max\ \phi(\lambda) \quad \text{s.t. } 0 \leq \lambda \leq 1, \tag{28}$$

where

$$\phi(\lambda) = \frac{\gamma_{A\mapsto B} - \gamma_E}{1+\gamma_E}, \tag{29}$$

which is due to the fact that $\log_2(1+\phi(\lambda))$ in (27) is a strictly increasing function w.r.t $\phi(\lambda)$, and thus (28) can be solved analytically in the high SNR regime as given in Theorem 3.

*Theorem 3: In large SNR regime, the function $\phi(\lambda)$ in (29) is proven to be quasi-concave w.r.t $\lambda$ in the feasible set where $0 \leq \lambda \leq 1$ and $\lambda^\star$ can be obtained as*

$$\lambda^\star = \frac{1}{1+\sqrt{\nu}}, \nu \geq 1 \tag{30}$$

*where $\nu = \frac{L_{au}S_{au}}{L_{ub}S_{ub}} + \frac{L_{ae}S_{ae}}{L_{be}S_{be}}$.*

*Proof:* See Appendix C. ∎

$$\begin{aligned} P_c = {} & 2(1+K_{ub})e^{-K_{au}-K_{ub}} \exp\left(-\frac{(1+K_{au})(1-\beta+\zeta)N_0\delta_t}{(1-\beta)P_aL_{au}}\right) \\ & \times \sum_{d=0}^{D}\sum_{u=0}^{d}\sum_{s=0}^{u}\sum_{r=0}^{R} \frac{\Gamma(D+d)D^{1-2\,d}\Gamma(R+r)R^{1-2r}}{\Gamma(D-d+1)\Gamma(d+1)\Gamma(u-s+1)\Gamma(s+1)} \\ & \times K_{au}^d(K_{au}+1)^u K_{ub}^r(1+K_{ub})^{\frac{r+u-s-1}{2}} \left(\frac{(1-\beta+\zeta)N_0\delta_t}{(1-\beta)P_aL_{au}}\right)^s \left(\frac{N_0\delta_t}{\varepsilon\beta P_aL_{au}L_{ub}}\right)^{u-s} \\ & \times \mathrm{I}_{r+s-u+1}\left(2\sqrt{\frac{(1+K_{au})(1+K_{ub})N_0\delta_t}{\varepsilon\beta P_aL_{au}L_{ub}}}\right), \end{aligned} \tag{21}$$

$$\begin{aligned} \mathcal{L}_2 = {} & 1 - \frac{2(1+K_{ue})e^{-(K_{au}+K_{ub}+K_{ue})}}{\sqrt{K_{ub}\left(1+\delta_e\frac{(1+K_{au})P_bL_{ub}}{(1+K_{ub})P_aL_{au}}\right)}} \exp\left(\frac{K_{ub}/2}{\left(1+\delta_e\frac{(1+K_{au})P_bL_{ub}}{(1+K_{ub})P_aL_{au}}\right)} - \frac{(1+K_{ue})(1-\beta+\zeta)\delta_eN_0}{(1-\beta)P_aL_{au}}\right) \\ & \times \sum_{d=0}^{D}\sum_{u=0}^{d}\sum_{r=0}^{u}\sum_{q=0}^{Q}\sum_{s=0}^{u-r} \Theta(D,Q,d,q,u,r,s)K_{ue}^q(1+K_{ue})^{u+q-s}K_{au}^d\mathrm{M}_{-(r+\frac{1}{2}),0}\left(K_{ub}+(1+K_{au})\delta_eP_bL_{ub}\right) \\ & \times \left(\frac{1}{1+\left(\delta_e\frac{(1+K_{au})P_bL_{ub}}{(1+K_{ub})P_aL_{au}}\right)^{-1}}\right)^r \left(\frac{\delta_eN_0}{\varepsilon\beta P_aL_{au}L_{ue}}\right)^{u-r-s} \left(\frac{(1-\beta+\zeta)\delta_eN_0}{(1-\beta)P_aL_{au}}\right)^s \left(\frac{\delta_e\,N_0}{\varepsilon\,\beta\,P_a\,L_{au}\,L_{ue}}\right)^{\frac{q+s+1}{2}} \\ & \times \mathrm{K}_{q+s+1}\left(\sqrt{\frac{\delta_e\,N_0}{\varepsilon\,\beta\,P_a\,L_{au}\,L_{ue}}}\right), \end{aligned} \tag{25}$$

where

$$\Theta(D,Q,d,q,u,r,s) = \frac{Q^{1-2\,q}D^{1-2\,d}\Gamma\,(s+1)\,\Gamma\,(Q+q)\,\Gamma\,(D+d)}{\Gamma\,(s-u+r+1)\,(\Gamma\,(u-r+1))^2\,\Gamma\,(Q-q+1)\,\Gamma\,(D-d+1)\,(\Gamma\,(q+1))^2\,\Gamma\,(d+1)} \tag{26}$$

### D. ACHIEVABLE AVERAGE SECRECY RATE

*Definition 3: The achievable average secrecy rate (ASR) is defined as*

$$\bar{C}_S \triangleq \mathbb{E}\{C_S\}, \tag{31}$$

*Averaging over all realizations of the channels yields $\bar{C}_S$ in (32), as shown at the bottom of this page.*

Owning to the fact that the exact computation of (32) is an arduous task and hence, instead, we derive a tight lower-bound for ASR in the Theorem below. First, we present the following worthwhile lemma, by which we then delve into the derivation of the closed-form lower-bound for the ASR in Theorem 4.

*Lemma 1: Let $X$ be a non-central chi-square random variable with two degrees of freedom and the non-centrality parameter $\lambda$, also $b$ holds non-negative values, then the expectation of the new random variable $Y = \ln(X + b)$, can be obtained as follows.*

$$\mathbb{E}\{\ln(X+b)\} = \int_0^\infty \frac{1}{2}\ln(x+b)e^{-\frac{x+\lambda}{2}}I_0(\sqrt{\lambda x})dx \triangleq \begin{cases} g_1(\lambda), & \text{for } b=0 \\ g_2(\lambda, b), & \text{for } b>0 \end{cases} \tag{33}$$

*where $g_1(\cdot)$ and $g_2(\cdot,\cdot)$ are defined respectively as*

$$g_1(x) \overset{(a)}{=} \exp(-\frac{x}{2})\sum_{r=0}^{R} L_r x^r,$$
$$g_2(x,b) \overset{(b)}{=} \exp\left(-\frac{x}{2}\right)\sum_{r=0}^{R} C_r(b)x^r, \tag{34}$$

*where $R$ is some positive integer and the coefficients $L_r$ and $C_r(b)$ are given, as finite series, respectively, by*

$$L_r = \frac{\Gamma(R+r)R^{1-2r}(\Psi(r+1)+\ln 2)}{\Gamma(r+1)\Gamma(R-r+1)2^r}, \tag{35}$$

*and*

$$C_r(b) = \frac{\Gamma(R+r)R^{1-2r}\Phi(r,b)}{\Gamma(r+1)^2\Gamma(R-r+1)4^r}, \tag{36}$$

*wherein $\Gamma(\cdot)$ and $\Psi(\cdot)$ are the Gamma function and the Psi function respectively defined as $\Gamma(x) \triangleq \int_0^\infty t^{x-1}e^{-t}dt$ and $\Psi(x) \triangleq \frac{d}{dx}\Gamma(x)$ [34]. Moreover, the function $\Phi(\cdot,\cdot)$ in (36) is given by (37), as shown at the bottom of the this page, wherein $G_{p,q}^{a,b}\left(\begin{matrix}\mathbf{a},\mathbf{b}\\ \mathbf{p},\mathbf{q}\end{matrix}\middle| x\right)$ is the analytical MeijerG function and a few first terms of $G_{2,3}^{3,0}\left(\begin{matrix}1,1\\ 0,0,j+1\end{matrix}\middle|\frac{b}{2}\right)$ are given in Table 1 wherein $\mathrm{Ei}(\cdot)$ represents one-argument exponential integral defined as $\mathrm{Ei}(x) = \int_{-\infty}^{x}\frac{e^t}{t}dt$. Besides, $\Gamma(x,a) \triangleq \int_x^\infty e^{-t}t^{a-1}dt$ is the upper incomplete Gamma function [34]. It should be noted that (a) and (b) are respectively obtained by applying [34, Eq. (4.352.1)] and [34, Eq. (8.352.2)] to calculate the integral expression given in (33), and after tedious mathematical manipulations.*

**TABLE 1.** Some equivalent expressions for the function $G_{2,3}^{3,0}\left(\begin{matrix}1,1\\ 0,0,j+1\end{matrix}\middle|\frac{b}{2}\right)$.

| $j$ | $G_{2,3}^{3,0}\left(\begin{matrix}1,1\\ 0,0,j+1\end{matrix}\middle|\frac{b}{2}\right)$ |
|---|---|
| 0 | $-\mathrm{Ei}(-\frac{b}{2})$ |
| 1 | $-\mathrm{Ei}(-\frac{b}{2})+\exp\left(-\frac{b}{2}\right)$ |
| 2 | $-2\mathrm{Ei}(-\frac{b}{2})+\left(\frac{b}{2}+3\right)\exp\left(-\frac{b}{2}\right)$ |
| 3 | $-6\mathrm{Ei}(-\frac{b}{2})+\left(\frac{b^2}{4}+\frac{5b}{2}+11\right)\exp\left(-\frac{b}{2}\right)$ |
| 4 | $-24\mathrm{Ei}(-\frac{b}{2})+\left(\frac{b^3}{8}+\frac{7b^2}{4}+13b+50\right)\exp\left(-\frac{b}{2}\right)$ |

*Theorem 4: The lower bound of the average secrecy rate of the proposed secure UAV-enabled relaying system is given by*

$$\bar{C}_{LB} = \frac{1}{2\ln 2}\Big[\ln(1+\exp(T_1)) - \ln(1+T_2)\Big]^+, \tag{38}$$

*with*

$$T_1 \triangleq \ln\left(\frac{(1-\beta)P_aL_{au}}{(1-\beta+\zeta)N_0}\right) + g_1(\lambda_{au}) + g_1(\lambda_{ub}) - g_2\left(\lambda_{ub}, \frac{1-\beta}{\varepsilon\beta(1-\beta+\zeta)L_{ub}}\right), \tag{39}$$

$$T_2 \triangleq \frac{\varepsilon\beta P_a(\lambda_{au}+2)}{\varepsilon\beta P_b(\lambda_{bu}+2)+\varepsilon\beta(1+\frac{\zeta}{1-\beta})N_0+\frac{N_0}{(\lambda_{ue}+2)}} + \frac{P_a}{P_b}\frac{L_{ae}}{L_{be}}\exp\left(\frac{N_0}{P_bL_{be}}\right)\mathrm{E}_1\left(\frac{N_0}{P_bL_{be}}\right). \tag{40}$$

*Proof:* See Appendix D. ■

$$\bar{C}_S = \mathbb{E}\left\{\Big[\frac{1}{2}\log_2(1+\gamma_{A\mapsto B}) - \frac{1}{2}\log_2(1+\gamma_E)\Big]^+\right\} = \frac{1}{2\ln 2}\int_{x=0}^\infty\int_{y=0}^\infty\int_{z=0}^\infty\int_{v=0}^\infty\int_{w=0}^\infty\left[\ln\left(\frac{1+\gamma_{A\mapsto B}}{1+\gamma_E}\right)\right]^+ f_{X,Y,Z,V,W}(x,y,z,v,w)dxdydzdvdw, \tag{32}$$

$$\Phi(i,b) = \exp\left(\frac{b}{2}\right)\sum_{j=0}^{i}\binom{i}{j}(-b)^{i-j}2^j\left[G_{2,3}^{3,0}\left(\begin{matrix}1,1\\ 0,0,j+1\end{matrix}\middle|\frac{b}{2}\right) + \ln(b)\,\Gamma(j+1,\frac{b}{2})\right] \overset{(a)}{=} \sum_{j=0}^{i}\sum_{k=0}^{j}(-1)^i\binom{i}{j}\left(\frac{2}{b}\right)^j\left[e^{b/2}G_{2,3}^{3,0}\left(\begin{matrix}1,1\\ 0,0,j+1\end{matrix}\middle|\frac{b}{2}\right) + \ln(b)\binom{j}{k}(j-k)!\left(\frac{b}{2}\right)^k\right] \tag{37}$$

### E. ASYMPTOTIC ASR ANALYSIS

We now provide the asymptotic analysis of the ASR, i.e., the ASR performance when transmit SNR $\rho \triangleq \frac{P}{N_0}$ goes to infinity. To this aim, according to the definition in [35], the high SNR slope $S_\infty$ and the high SNR power offset $L_\infty$ are obtained, respectively, as

$$S_\infty = \lim_{\rho\to\infty} \frac{\bar{C}_s}{\log_2 \rho} = \frac{1}{2}, \quad \text{bps/Hz/(3dB)} \tag{41}$$

and

$$\begin{aligned} L_\infty &= \lim_{\rho\to\infty} \left( \log_2 \rho - \frac{\bar{C}_s}{S_\infty} \right), \quad \text{(3dB)} \\ &\approx \log_2\left(1+\frac{\lambda}{(1-\lambda)}\left[\frac{2L_{ae}}{L_{be}}+\frac{L_{au}}{L_{ub}}\left(1+\frac{2K_{au}+1}{(K_{au}+1)^2}\right)\right]\right) \\ &\quad + \frac{2K_{au}+1}{2\ln 2(K_{au}+1)^2} + \frac{2K_{ub}+1}{2\ln 2(K_{ub}+1)^2} \\ &\quad + \log_2\left(\frac{(1+\varepsilon\beta)(1-\beta)+\zeta^2\beta}{\varepsilon\beta(1-\beta)\lambda L_{au}L_{ub}}\right). \end{aligned} \tag{42}$$

*Proof:* See Appendix E. ∎

Based on the closed-form expressions in (41) and (42), we note that the high-SNR measures $S_\infty$ and $L_\infty$ explicitly capture the impact of distance-dependent channel features and system parameters. By doing so, the ASR in the high-SNR regime is expanded as an affine function given below, demonstrating the scaling and power required for the specific ASR of interest.

$$\bar{C}_s \approx S_\infty \left( \frac{\rho[dB]}{3\text{dB}} - L_\infty \right). \tag{43}$$

Remarkedly, the high-SNR slope $S_\infty$ in (41) sheds light on the fact that for the two-hop UAV-relaying, the channel fading has zero impact on the ASR slope, which in our setting corresponds to the maximum multiplexing gain of the network. Interestingly, we also observe from (42) that the links between UAV and the legitimate nodes play a significant role in the high-SNR power offset, so do power allocation and power splitting parameters. This illustrates that an appropriate UAV positioning between source and destination leads to a reduced $L_\infty$ which further results in improvement of the ASR performance based on the expression given by (43).

## V. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we present simulation results of connection probability, secrecy outage probability, and average secrecy rate in order to validate our theoretical results in the paper. We also demonstrate both reliability and security performance enhancements offered by the proposed UAV-relaying (UR) with destination-assisted CJ transmission protocol, compared to the case using a ground node as a relay which located with the same horizontal distance from the legitimate nodes, namely the GR scheme, and the case using UR but without destination jamming as two competitive benchmarks for the sake of comparison.

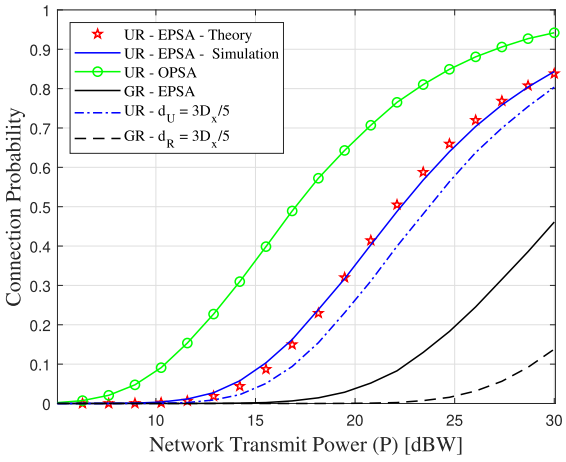


**FIGURE 5.** Connection Probability vs. Network Transmit Power.

Unless otherwise stated, we consider the following system parameters in all simulations. We assume $D_x = 10$ (the normalized distance of $\mathbb{A}$-$\mathbb{B}$ w.r.t 100m), $H = 1.5$ (the normalized height at which UAV operates w.r.t 100m). We assume the nodes locations: $W_A = (0, 0, 0)$, $W_B = (D_x, 0, 0)$, $W_E = (\frac{4D_x}{5}, 1, 0)$, $W_U = (\frac{D_x}{5}, 0, H)$. The path-loss exponents are $\alpha_L = 2$ and $\alpha_N = 3.5$, respectively. Besides, the network transmission rate $R_t = 0.5$ bps/Hz, the secrecy rate $R_s = 0.2$ bps/Hz are adopted. Further, we assume $N_0 = 10$dBm, $\zeta = 2$, energy harvesting efficiency factor $\varepsilon = 0.7$, $\omega_1 = 0.28$, $\omega_2 = 9.61$, $\kappa_m = 1$, and $\kappa_M = 10$ as [27], [30], [36]. Also, the EPSA represents the case of the equal power allocation corresponding to $\lambda = 0.5$ and the equal power splitting ratio; i.e., $\beta = 0.5$. The Monte-Carlo simulation are obtained through averaging over 100, 000 realizations of the channel coefficients.

Fig. 5 is provided to illustrate the CP performance for the proposed transmission protocol against the network transmit power $P$. Here, OPSA refers to the case with optimal values obtained in (20) for a given $P$, $d_U$ represents the horizontal projection distance of $\mathbb{U}$ to $\mathbb{A}$, and $d_R$ is the distance from the ground relay, in the conventional GR scheme, to source. Here, for a fair comparison, we assume $d_U = d_R$. We can observe that the CP of OPSA-based scheme gets approximately doubled, compared to EPSA-based one, in the practical range of transmit power, e.g., for $P = 20$ dBW. The figure also compares the simulated CP using (18) and theoretical CP using (21) of the proposed protocol with the EPSA setting, demonstrating that the both curves are well matched which validates our theoretical results. Fig. 5 also illustrates a significant CP improvement of the proposed protocol, when compared to the conventional GR scheme, under the similar setting with EPSA.

Fig. 6 illustrates the simulated and theoretical SOP versus network transmit power $P$ for the proposed protocol using CJ with $\lambda = 0.7$ and demonstrates they are well matched. The figure also compares the proposed protocol, the UAV-based relaying without any security technique and the

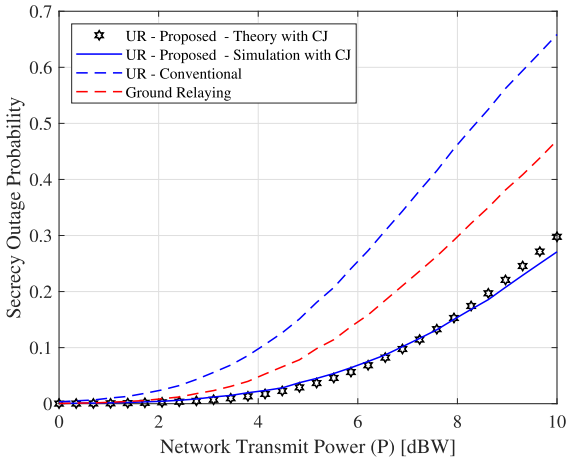


**FIGURE 6.** Secrecy Outage Probability vs. Network Transmit Power.

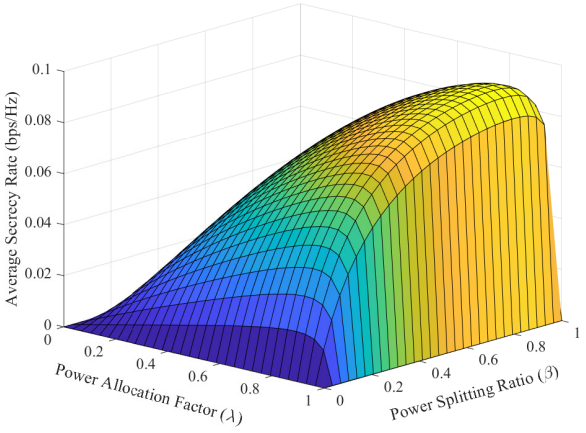


**FIGURE 8.** Average Secrecy Rate vs. Power Allocation Factor and Power Splitting Ratio.

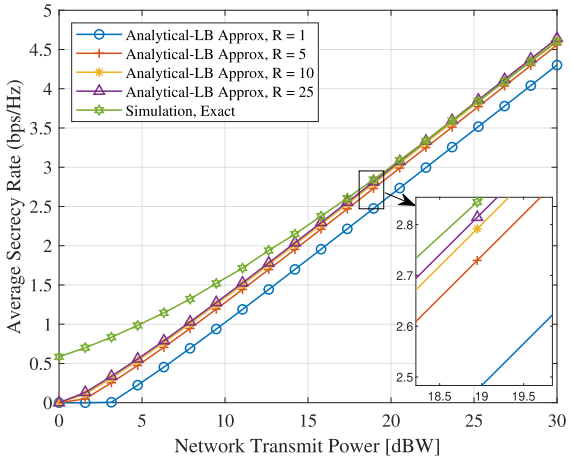


**FIGURE 7.** Average Secrecy Rate vs. Network Transmit Power.

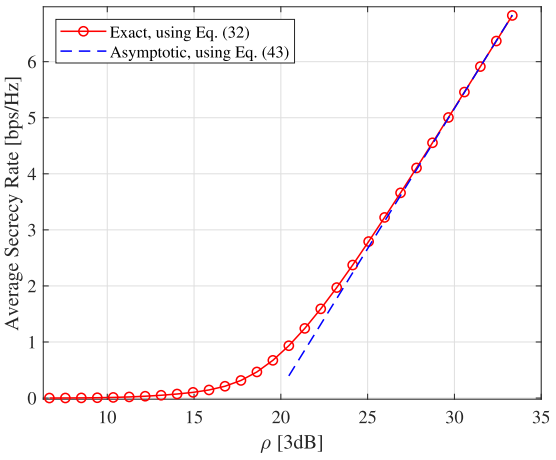


**FIGURE 9.** Exact versus Asymptotic ASR. we set $\lambda = 0.5$, $\beta = 0.5$.

one using ground relaying, and demonstrates the effectiveness of our protocol in terms of SOP thanks to the joint effect of destination CJ and SWIPT.

Fig. 7 compares the lower bound of ASR (see Theorem 4) with different truncated values $R$ (see Theorem 4) and the simulated result using the exact expression (32). We can see that they are very close, especially when $P \geq 17$dBW. Further, we observe that normalizing the gap between the exact value and the lower bound w.r.t the exact value yields the relative errors of 0.0907, 0.0617, and 0.0512 for the cases of $R = 5$, $R = 10$, and, $R = 25$, respectively. This demonstrates the finite series we obtained are acceptably valid while explicitly truncated.

Fig. 8 depicts the impact of $\lambda$ and $\beta$ on ASR. Given a fixed power budget $P = 20$ dBW, the ASR increases when $\lambda$ and $\beta$ increase. The best ASR can be obtained at $\lambda = 0.83$ and $\beta = 0.8$. A higher $\lambda$ (i.e., higher $P_a$) provides higher reliability of data transmission, but when $\lambda > 0.83$, ASR decreases slightly. This is due to the fact that a high source power can enhance $C_M$ and a low jamming power is sufficient to degrade eavesdropper. Overall, the plot provides a good trade-off between source power and destination jamming power in terms of ASR. Further, Fig. 9 compares the exact $\bar{C}_s$ in (32) vs asymptotic ASR $\bar{C}_s$ in (43) and demonstrates their agreement when $\rho \geq 25$dB. This also validates the accuracy of high-SNR measures $S_\infty$ and $L_\infty$ derived for the asymptotic case in Section IV-E.

Fig. 10 shows ASR against normalized horizontal distance of the proposed protocol with and without destination CJ for different $\lambda$ values. Here normalized horizontal distance is defined as the ratio of the horizontal distance of ($\mathbb{A}$-$\mathbb{U}$) to that of ($\mathbb{A}$-$\mathbb{B}$). This scenario can be viewed as a relay moving from the initial location above $\mathbb{A}$ with a direct path to the final location right above $\mathbb{B}$ and we are seeking the best location of $\mathbb{U}$ in terms of ASR.

From Fig. 10, we observe that the proposed protocol with CJ outperforms the one without CJ, and particularly, the proposed protocol with CJ and $\lambda^*$ leads to the best ASR, compared to other $\lambda$ values, over all different normalized horizontal distances. Also, we observe the best location of $\mathbb{U}$ is $0.9D_x$. This is due to the fact that when $\mathbb{U}$ is near $\mathbb{B}$and far from $\mathbb{A}$, we need to allocate more $P_a$ to enhance $C_M$ for source transmission and less $P_b$, which is sufficient for destination CJ. When $\mathbb{U}$ is at the location

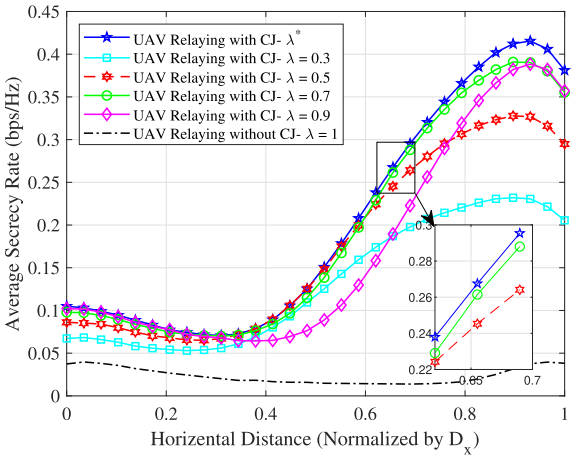


**FIGURE 10.** Average Secrecy Rate versus Horizontal Distance Ratio.

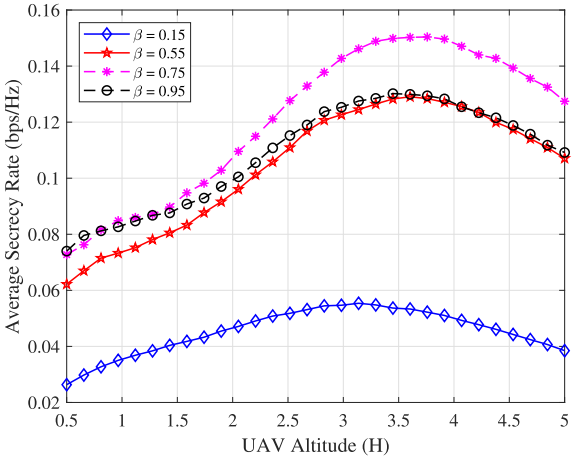


**FIGURE 11.** Average Secrecy Rate versus Normalized UAV Altitude.

of $0.2D_x - 0.5D_x$ (i.e., $\mathbb{U}$ is in the vicinity of eavesdropper), the wiretap link obviously reduces the ASR. Last but not least, when $\mathbb{U}$ is within $(0.35D_x, 0.65D_x)$, more proportion of the power budget should be dedicated for jamming in order to improve ASR.

Fig. 11 displays ASR against UAV altitude $H$ for the proposed protocol with different $\beta$. Firstly, we observe that $\beta = 0.75$ and $H = 3.5$ yield the best ASR among all. Secondly, we observe, when $H$ increases till 3.5, ASR increases to the peak, and after that, ASR decreases. This is due to the fact that, from $H = 3.5$ onwards, the attenuation factor caused by the $\mathbb{U}$'s long distance from the ground nodes significantly affects the ASR. When $0 < H \leq 3.5$, the ASR is a quasi-concave function having one optimal value for given system parameters. Furthermore, for $\mathbb{U}$ is in low altitude, e.g., $H = 0.6$, increasing $\beta$ (i.e., a larger proportion of the received power is stored for EH which is then utilized in AF relaying), yields improved ASR. For higher altitudes, the ASR increases if $0 < \beta < \beta^*$, or decreases if $\beta^* < \beta < 1$, where $\beta^* = 0.75$. This is due to the fact that, when $\beta > \beta^*$, large UAV transmission power can lead to the improved received SNR at $\mathbb{B}$, but this also yields better signal reception at Eve.

## VI. CONCLUSIONS

In this paper, we proposed a secure and energy-efficient source-UAV-destination transmission protocol with the aid of destination CJ and SWIPT at the UAV-relay, when a passive ground eavesdropper exists. We derived the connection probability, secrecy outage probability, instantaneous secrecy rate, and average secrecy rate of the proposed transmission protocol from $\mathbb{A}$ to $\mathbb{B}$ through a stationary $\mathbb{U}$ and corroborated them via simulations. Moreover, the high-SNR secrecy measures of the ASR metric were discussed, both mathematically and also from an engineering standpoint, in terms of the high-SNR power offset and the high-SNR slope. Further, by simulations, we demonstrated significant performance improvement of our protocol, when compared to the-state-of-the-art benchmarks, namely conventional GR and UR with/without CJ transmission protocols. We also identified the best location of $\mathbb{U}$ that provides the optimal ASR, given a fixed eavesdropper location. Finally, we evaluated the impacts of different system parameters on the secrecy and reliability performances; specifically, we obtained the optimal power allocation factor and the optimal power splitting ratio to improve the secrecy throughput and reliability of the network. For future work, we will consider the extension to flying UAV-relaying with extra degrees of freedom in the system design focusing on the optimization of the communications resources and path-planning.

## APPENDIX A
## DERIVATION OF CONNECTION PROBABILITY

The connection probability $P_c$ given by (18) can be obtained as follows (see (A.1)), as shown at the bottom of the next page, where $X \triangleq L_{au}S_{au}$, $Y \triangleq L_{ub}S_{ub}$,

$$A \triangleq \frac{(1-\beta+\zeta)N_0\delta_t}{(1-\beta)P_aL_{au}} \quad B \triangleq \frac{N_0\delta_t}{\varepsilon\beta P_aL_{au}L_{ub}}$$

and $\mathrm{Q}(a, b)$ is the first-order Marqum Q-function, and $\mathrm{I}_\nu(\cdot)$ is the modified Bessel function of the first kind with $\nu$th order. Furthermore, $(a)$ follows from plugging the approximate expressions for $Q(\cdot,\cdot)$ and $I_0(\cdot)$ given respectively as [37]

$$I_0(y) = \sum_{r=0}^{R} \frac{\Gamma(R+r)R^{1-2r}}{\Gamma^2(r+1)\Gamma(R-r+1)} \left(\frac{y}{2}\right)^{2r}, \quad \text{(A.2)}$$

and

$$\mathrm{Q}(x,y) = \sum_{d=0}^{D}\sum_{u=0}^{d} \frac{\Gamma(D+d)D^{1-2d}x^{2d}y^{2u}}{\Gamma(D-d+1)d!u!2^{d+u}} e^{-\frac{x^2+y^2}{2}}, \quad \text{(A.3)}$$

Finally, applying the equation [34, Eq. (3.471.9)] for calculating the integral expression of the last equation of (A.1), one can reach, after tedious manipulations, at (21) and so the proof is done.

## APPENDIX B
## DERIVATION OF SECRECY OUTAGE PROBABILITY

To obtain $P_{so}$ we need to calculate $\mathcal{L}_1$ and $\mathcal{L}_2$. Henceforth, in order to calculate $\mathcal{L}_1$, let define $S_{ae} \triangleq V$ and $S_{be} \triangleq W$ while rewriting (24) as

$$\begin{aligned}\mathcal{L}_1 &= \Pr\left\{V < \frac{P_b L_{be}\delta_e}{P_a L_{ae}} W + \frac{N_0\delta_e}{P_a L_{ae}}\right\} \\ &= \mathbb{E}_W\left\{F_{V|W}\left(\frac{P_b L_{be}\delta_e}{P_a L_{ae}} w + \frac{N_0\delta_e}{P_a L_{ae}}\right)\right\} \\ &= 1 - \int_0^\infty \exp\left(-\left[\frac{P_b L_{be}\delta_e}{P_a L_{ae}} + 1\right] w - \frac{N_0\delta_e}{P_a L_{ae}}\right) dw, \quad \text{(B.1)}\end{aligned}$$

calculating the last integral results in (24).

Now, we focus on obtaining an analytical expression for $\mathcal{L}_2$ as follows. By defining the auxiliary variables $a_1 \triangleq \delta_e \frac{P_b L_{ub}}{P_a L_{au}}$, $a_2 \triangleq \delta_e \frac{N_0}{\varepsilon\beta P_a L_{au} L_{ue}}$, $a_3 \triangleq \delta_e \frac{(1-\beta+\zeta)N_0}{(1-\beta)P_a L_{au}}$, and letting $X \triangleq S_{au}$, $Y \triangleq S_{ub}$, and $Z \triangleq S_{ue}$, one can rewrite $\mathcal{L}_2$ given in (25) as

$$\begin{aligned}\mathcal{L}_2 &= \Pr\{X \le a_1 Y + a_2 Z^{-1} + a_3\} \\ &= \mathbb{E}_Z\{\mathbb{E}_{Y|Z}\{F_{X|Y,Z}(a_1 y + a_2 z^{-1} + a_3)\}\} \\ &= 1 - \int_0^\infty \Xi(z) f_Z(z) dz, \quad \text{(B.2)}\end{aligned}$$

where $\Xi(z) \triangleq \int_0^\infty \mathrm{Q}\left(\sqrt{a}, \sqrt{by + c(z)}\right) f_Y(y) dy$ in which $a \triangleq 2K_{au}$, $b \triangleq 2(1+K_{au})a_1$, $c(z) \triangleq 2(1+K_{au})(a_2\, z^{-1} + a_3)$. Then, $\Xi(z)$ is calculated in a closed-form expression using (A.3) given in Appendix A as (see (B.3)), as shown at the bottom of the next page. in which $\tilde{b} \triangleq \frac{b}{2} + K_{ub} + 1$, $\tilde{c} \triangleq \sqrt{K_{ub}(1+K_{ub})}$. Moreover, $(b)$ comes from using [34, Eq. (6.643.2)] to calculate the integral term, wherein $\mathrm{M}(\cdot)$ is the Whittaker M-function. Next, in order to obtain a closed-form expression for the single-form integral given by (B.2) we further calculate as (see (B.4)), as shown at the bottom of the next page, where $c_1 \triangleq K_{ue}(K_{ue}+1)$, $b_1 \triangleq K_{ue}+1$, $b_2 \triangleq 2(K_{ue}+1)a_3$, $b_3 \triangleq 2(K_{ue}+1)a_2$, and $\mathrm{K}_\nu(\cdot)$ denotes the modified Bessel function with the second kind and $\nu$-th order. Note that the above equation achieved by applying [34, Eq. (3.478.4)]. Finally, through tedious mathematical manipulations we can achieve the closed-form expression for the SOP given by (25), and hence, the proof is done.

## APPENDIX C
## DERIVATION OF OPTIMAL $\lambda^\star$

Taking the auxiliary variables

$$\begin{aligned}c_1 &\triangleq \frac{\varepsilon\beta(1-\beta)PXY}{\varepsilon\beta(1-\beta+\zeta)YN_0 + (1-\beta)N_0}, c_2 \triangleq \frac{PV}{N_0} \\ c_3 &\triangleq \frac{PW}{N_0}, c_4 \triangleq \frac{\varepsilon\beta(1-\beta)PXZ}{\varepsilon\beta(1-\beta+\zeta)ZN_0 + (1-\beta)N_0} \\ c_5 &\triangleq \frac{\varepsilon\beta(1-\beta)PYZ}{\varepsilon\beta(1-\beta+\zeta)ZN_0 + (1-\beta)N_0}\end{aligned}$$

where $X \triangleq L_{au}S_{au}$, $Y \triangleq L_{ub}S_{ub}$, $Z \triangleq L_{au}S_{ue}$, $V \triangleq L_{ae}S_{ae}$, and $V \triangleq L_{ae}S_{ae}$ are defined, we rewrite the function $\Phi(\lambda)$, considering high transmit SNR approximation, as

$$\Phi(\lambda) \approx \frac{c_1 c_3 c_5 \lambda(\lambda-1)^2}{b_2\lambda^2 + b_1\lambda + b_0}, \quad \text{(C.1)}$$

where $b_2 = (c_4 - c_5)c_3 + c_2c_5$, $b_1 = (2c_5 - c_4)c_3 - c_2c_5 - c_2 - c_4$, $b_0 = -c_3c_5$. Now, taking the first derivation of the function $\Phi$ w.r.t $\lambda$, i.e., $\Phi_1(\lambda) \triangleq \frac{d\Phi(\lambda)}{d\lambda}$ results a rational polynomial function with always-positive denominator and the numerator of forth-order, where it can readily be found that 0 and 1 are the roots of both $\Phi(\lambda)$ and its first derivative $\Phi_1(\lambda)$. Hence the remained two roots are the solutions of the second order polynomial given as

$$(\nu-1)\lambda^2 + 2\lambda - 1 = 0 \quad \text{(C.2)}$$

where $\nu = \frac{c_2c_5 + c_3c_4}{c_3c_5}$. As such, considering the feasible set of $0 \le \lambda \le 1$, we have three cases as

1) $\nu < 1$, no optimum solution
2) $\nu = 1$, $\lambda^\star = \frac{1}{2}$
3) $\nu > 1$, $\lambda^\star = \frac{1}{1+\sqrt{\nu}}$

Furthermore, note that it is easy to prove $\Phi_1(\lambda)$ holds positive values in $(0, \lambda^\star]$ and are negative in $(\lambda^\star, 1)$ and the extremum determines the maximum of the $\Phi(\lambda)$ [38], and hence the proof is complete.

## APPENDIX D
## DERIVATION OF LOWER-BOUNDED ASR

In order to obtain a closed-form lower-bound expression for $\mathbb{E}\{C_S\}$, one can write, following the Jensen's inequality,

$$\begin{aligned}P_c &= \Pr\left\{X > A + \frac{B}{Y}\right\} = 1 - \mathbb{E}_Y\left\{F_{X|Y}\left(A + \frac{B}{Y}\right)\right\} \\ &= (1+K_{ub})e^{-K_{ub}} \int_0^\infty \mathrm{Q}\left(\sqrt{2K_{au}}, \sqrt{2(1+K_{au})\left(A + \frac{B}{y}\right)}\right) e^{-(1+K_{ub})y} \mathrm{I}_0\left(2\sqrt{K_{ub}(1+K_{ub})}\sqrt{y}\right) dy \\ &\overset{(a)}{=} (1+K_{ub})e^{-K_{au}-K_{ub}-(1+K_{au})A} \sum_{d=0}^{D}\sum_{u=0}^{d}\sum_{s=0}^{u} \frac{\Gamma(D+d)D^{1-2\,d}\Gamma(R+r)K_{au}^d(K_{au}+1)^u A^s B^{u-s}\binom{u}{s}}{\Gamma(D-d+1)\Gamma(d+1)\Gamma(u-s+1)\Gamma(s+1)} \\ &\quad \times \int_0^\infty y^{-(u-s)} \exp\left(-(1+K_{ub})y - (1+K_{au})\frac{B}{y}\right) \mathrm{I}_0\left(2\sqrt{\{K_{ub}(1+K_{ub})y\}}\right) dy, \quad \text{(A.1)}\end{aligned}$$

as [25] (see (D.1)), as shown at the bottom of this page. In (D.1), the term $\mathbb{E}\{\ln(\gamma_{A\mapsto B})\}$ is further calculated as

$$\mathbb{E}\{\ln(\gamma_{A\mapsto B})\} \geq \ln\left(\frac{(1-\beta)P_aL_{au}}{(1-\beta+\zeta)N_0}\right) + \mathbb{E}\{\ln(S_{au}S_{ub})\} - \mathbb{E}\left\{\ln\left(S_{ub}+\frac{1-\beta}{\varepsilon\beta(1-\beta+\zeta)L_{ub}}\right)\right\} \triangleq T_1, \tag{D.2}$$

where $T_1$ can be analytically obtained using Lemma 1 as given in (39). Letting $T_2 \triangleq \mathbb{E}\{\gamma_E^{(1)}\} + \mathbb{E}\{\gamma_E^{(2)}\}$, the remained parts $\mathbb{E}\{\gamma_E^{(1)}\}$ and $\mathbb{E}\{\gamma_E^{(2)}\}$ in (D.1) are derived as

$$\mathbb{E}\{\gamma_E^{(1)}\} = \frac{P_a}{P_b}\frac{L_{ae}}{L_{be}}\exp\left(\frac{N_0}{P_bL_{be}}\right)\mathrm{E}_1\left(\frac{N_0}{P_bL_{be}}\right), \tag{D.3}$$

where $\mathrm{E}_1(\cdot) = \int_1^\infty e^{-tx}t^{-a}dx$ is the exponential integral, $(b)$ follows from the approximate given in [39] along considering the tight lower bound for $E\left\{\frac{1}{X}\right\}$ given in [40]. However that $E\left\{\frac{1}{X}\right\}$ can be readily obtained inasmuch as it equals to the first derivative of $g_1(x)$, already given in (34), w.r.t $x$, we use this tight approximation for simplicity.

## APPENDIX E
## DERIVATION OF HIGH SNR MEASURES

At high-SNR when $\rho$ goes to infinity, we have the following approximations

$$\gamma_{A\to B} \approx \frac{b_1S_{au}}{b_2+S_{ub}^{-1}}, \quad \gamma_E^{(1)} \approx a_1\frac{S_{ae}}{S_{be}}, \ \gamma_E^{(2)} \approx a_2\frac{S_{au}}{S_{bu}}, \tag{E.1}$$

where $a_1 = \frac{\lambda L_{ae}}{(1-\lambda)L_{be}}$, $a_2 = \frac{\lambda L_{au}}{(1-\lambda)L_{bu}}$, $b_1 = \varepsilon\beta\lambda L_{au}L_{ub}$, and $b_2 = \varepsilon\beta\left(1+\frac{\zeta}{1-\beta}\right)L_{ub}$ are defined. Now, commencing from the definition of $S_\infty$, we write as

$$S_\infty = \lim_{\rho\to\infty}\frac{\mathbb{E}\{C_s\}}{\log_2\rho} = \mathbb{E}\left\{\lim_{\rho\to\infty}\frac{\frac{1}{2}\log_2\left(\frac{1+\gamma_{A\to B}}{1+\gamma_E}\right)}{\log_2\rho}\right\} \approx \frac{1}{2}, \tag{E.2}$$

We now turn our focus on deriving $L_\infty$ as

$$L_\infty = \lim_{\rho\to\infty}\left(\log_2\rho - \frac{\mathbb{E}\{C_s\}}{S_\infty}\right) = \mathbb{E}\left\{\lim_{\rho\to\infty}\left(\log_2\rho - \frac{C_s}{S_\infty}\right)\right\}$$

$$\Xi(z) = \sum_{d=0}^{D}\sum_{u=0}^{d}\sum_{r=0}^{u}\frac{(1+K_{ub})e^{-K_{ub}}\Gamma(D+d)D^{1-2d}a^db^r\binom{u}{r}c^{u-r}\exp\left(-\frac{a+c}{2}\right)}{\Gamma(D-d+1)d!u!2^{d+u}} \times\int_0^\infty y^r\exp\left(-\left(\frac{b}{2}+K_{ub}+1\right)y\right)\mathrm{I}_0\left(2\sqrt{K_{ub}(1+K_{ub})}\sqrt{y}\right)dy$$

$$\overset{(b)}{=}\sum_{d=0}^{D}\sum_{u=0}^{d}\sum_{r=0}^{u}\frac{(1+K_{ub})e^{-K_{ub}}\Gamma(D+d)D^{1-2d}a^d(\frac{b}{\tilde{b}})^r\binom{u}{r}r!c^{u-r}}{\Gamma(D-d+1)d!u!2^{d+u}\tilde{c}\sqrt{\tilde{b}}} \times\exp(-\frac{a+c}{2}+\frac{\tilde{c}^2}{2\tilde{b}})\mathrm{M}_{-(r+\frac{1}{2}),0}(\frac{\tilde{c}^2}{\tilde{b}}), \tag{B.3}$$

$$\mathcal{L}_2 = 1-\sum_{d=0}^{D}\sum_{u=0}^{d}\sum_{r=0}^{u}\sum_{q=0}^{Q}\sum_{s=0}^{u-r}\frac{\Gamma(Q+q)Q^{1-2q}\Gamma(D+d)D^{1-2d}a^d(\frac{b}{\tilde{b}})^r\binom{u}{r}r!\binom{u-r}{s}b_3^{u-r-s}b_2^sc_1^q}{\Gamma(Q-q+1)\Gamma^2(q+1)\Gamma(D-d+1)d!u!2^{d+u-1}\tilde{c}\sqrt{\tilde{b}}} \times(1+K_{ub})(1+K_{ue})e^{-(K_{ub}+K_{ue})}\exp(-\frac{a}{2}+\frac{\tilde{c}^2}{2\tilde{b}}-\frac{b_2}{2})\left(\frac{b_3}{2b_1}\right)^{\frac{q+s+1}{2}} \times\mathrm{M}_{-(r+\frac{1}{2}),0}\left(\frac{\tilde{c}^2}{\tilde{b}}\right)\mathrm{K}_{q+s+1}\left(\sqrt{\frac{b_1b_3}{2}}\right), \tag{B.4}$$

$$\mathbb{E}\{C_S\} \geq \frac{1}{2\ln 2}\Big[\mathbb{E}\{\ln(1+\gamma_{A\mapsto B})\}-\mathbb{E}\{\ln(1+\gamma_E)\}\Big]^+ \geq \frac{1}{2\ln 2}\Big[\ln\left(1+\exp(\mathbb{E}\{\ln(\gamma_{A\mapsto B})\})\right)-\ln\left(1+\mathbb{E}\{\gamma_E^{(1)}\}+\mathbb{E}\{\gamma_E^{(2)}\}\right)\Big]^+, \tag{D.1}$$

$$\mathbb{E}\{\gamma_E^{(2)}\} \overset{(b)}{\approx} \frac{\varepsilon\beta(1-\beta)P_a(\lambda_{au}+2)(\lambda_{ue}+2)}{\varepsilon\beta(1-\beta)P_b(\lambda_{bu}+2)(\lambda_{ue}+2)+\varepsilon\beta(1-\beta+\zeta)(\lambda_{ue}+2)N_0+(1-\beta)N_0}, \tag{D.4}$$

$$= \mathbb{E}\left\{\log_2\left(1+2a_1\frac{S_{ae}}{S_{be}}+a_2\frac{S_{au}}{S_{bu}}\right)\right\} - \mathbb{E}\left\{\log_2\left(\frac{b_1 S_{au}}{b_2+S_{ub}^{-1}}\right)\right\}$$
$$\approx \log_2\left(1+2a_1+a_2\mathbb{E}\left\{\frac{S_{au}}{S_{bu}}\right\}\right) - \log_2\left(\frac{1+b_2}{b_1}\right) - \mathbb{E}\left\{\log_2 S_{au}S_{ub}\right\}, \quad \text{(E.3)}$$

Then, applying the fruitful Lemma given below to calculate the approximation of the expectations in the right-hand side of the last equation yields the closed-form expression given in (42).

*Lemma 2: Let $X$ and $Y$ be unit-mean RVs; i.e., $\mathbb{E}\{X\}=1$ and $\mathbb{E}\{Y\}=1$, which are distributed according to the non-central chi-square distribution with two degrees of freedom and K-factor parameters $K_x$ and $K_y$, respectively, whose PDF given by (2). The variance of $X$ is $\sigma_X^2=\frac{2K+1}{(K+1)^2}$. The expectation of new RVs $Z_1=\ln X$ and $Z_2=\frac{X}{Y}$ are given respectively as*

$$\mathbb{E}\{Z_1\} \overset{(a)}{=} (K+1)e^{-K} \times \sum_{r=0}^{R}\frac{\Gamma(R+r)R^{1-2r}K^r(\Psi(r+1)+\ln(K+1))}{\Gamma(r+1)\Gamma(R-r+1)} \overset{(b)}{\approx} -\frac{2K+1}{2(K+1)^2} \quad \text{(E.4)}$$

$$\mathbb{E}\{Z_2\} \overset{(c)}{\approx} 1+\frac{2K_x+1}{(K_x+1)^2} \quad \text{(E.5)}$$

*where (a) follows from [34, Eq. (4.352.2)], (b) and (c) each follows from applying the single and multivariate Taylor approximation for the moments of functions of RVs $\ln X$ and $\frac{X}{Y}$ around their means, respectively.*

## REFERENCES


[1] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[2] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2624–2661, 4th Quart., 2016.

[3] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV-relaying-assisted secure transmission with caching," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3140–3153, May 2019.

[4] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.

[5] X. Liu, Z. Li, N. Zhao, W. Meng, G. Gui, Y. Chen, and F. Adachi, "Transceiver design and multihop D2D for UAV IoT coverage in disasters," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1803–1815, Apr. 2019.

[6] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "UAV-enabled communication using NOMA," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 5126–5138, Jul. 2019.

[7] D. H. Choi, S. H. Kim, and D. K. Sung, "Energy-efficient maneuvering and communication of a single UAV-based relay," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 3, pp. 2320–2327, Jul. 2014.

[8] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.

[9] S. Zeng, H. Zhang, K. Bian, and L. Song, "UAV relaying: Power allocation and trajectory optimization using decode-and-forward protocol," in *Proc. IEEE ICC*, May 2018, pp. 1–6.

[10] M. Hua, Y. Wang, Z. Zhang, C. Li, Y. Huang, and L. Yang, "Outage probability minimization for low-altitude UAV-enabled full-duplex mobile relaying systems," *China Commun.*, vol. 15, no. 5, pp. 9–24, May 2018.

[11] M.-L. Ku, W. Li, Y. Chen, and K. J. R. Liu, "Advances in energy harvesting communications: Past, present, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1384–1412, 2nd Quart., 2016.

[12] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

[13] T. D. P. Perera, D. N. K. Jayakody, 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, 1st Quart., 2018.

[14] L. Yang, J. Chen, M. O. Hasna, and H.-C. Yang, "Outage performance of UAV-assisted relaying systems with RF energy harvesting," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2471–2474, Dec. 2018.

[15] Q. Wu, G. Y. Li, W. Chen, D. W. K. Ng, and R. Schober, "An overview of sustainable green 5G networks," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 72–80, Aug. 2016.

[16] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[17] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," 2019, *arXiv:1902.02472*. [Online]. Available: https://arxiv.org/abs/1902.02472

[18] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.

[19] Y. Cai, Z. Wei, R. Li, D. W. K. Ng, and J. Yuan, "Energy-efficient resource allocation for secure UAV communication systems," 2019, *arXiv:1901.09308*. [Online]. Available: https://arxiv.org/abs/1901.09308

[20] Y. Wang, W. Yang, X. Shang, and Y. Cai, "Energy-efficient secure transmission for UAV-enabled wireless powered communication," in *Proc. 10th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2018, pp. 1–5.

[21] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[22] M. T. Mamaghani and R. Abbas, "Security and reliability performance analysis for two-way wireless energy harvesting based untrusted relaying with cooperative jamming," *IET Commun.*, vol. 13, no. 4, pp. 449–459, 2019.

[23] M.-N. Nguyen, L. D. Nguyen, T. Q. Duong, and H. D. Tuan, "Real-time optimal resource allocation for embedded UAV communication systems," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 225–228, Feb. 2019.

[24] X. Sun, W. Yang, Y. Cai, Z. Xiang, and X. Tang, "Secure transmissions in millimeter wave SWIPT UAV-based relay networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 785–788, Jun. 2019.

[25] M. T. Mamaghani, A. Kuhestani, and K.-K. Wong, "Secure two-way transmission via wireless-powered untrusted relay and external jammer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8451–8465, Sep. 2018.

[26] R. Amorim, H. Nguyen, P. Mogensen, I. Z. Kovács, J. Wigard, and T. B. Sørensen, "Radio channel modeling for UAV communication over cellular networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 514–517, Aug. 2017.

[27] A. A. Khuwaja, Y. Chen, N. Zhao, M.-S. Alouini, and P. Dobbins, "A survey of channel modeling for UAV communications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2804–2821, 4th Quart., 2018.

[28] M. M. Azari, F. Rosas, K.-C. Chen, and S. Pollin, "Ultra reliable UAV communication using altitude and cooperation diversity," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 330–344, Jan. 2018.

[29] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3949–3963, Jun. 2016.

[30] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmWave networks using Matérn hardcore point processes," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1397–1409, Jul. 2018.

[31] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 341–355, Feb. 2018.

[32] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.
[33] J. Yao and J. Xu, "Secrecy transmission in large-scale UAV-enabled wireless networks," 2019, *arXiv:1902.00836*. [Online]. Available: https://arxiv.org/abs/1902.00836
[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*. New York, NY, USA: Academic, 2014.
[35] A. Lozano, A. M. Tulino, and S. Verdú, "High-SNR power offset in multiantenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134–4151, Dec. 2005.
[36] M. T. Mamaghani, A. Mohammadi, P. L. Yeoh, and A. Kuhestani, "Secure two-way communication via a wireless powered untrusted relay and friendly jammer," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.
[37] K. Cao and X. Gao, "Solutions to generalized integrals involving the generalized Marcum $Q$-function with application to energy detection," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1780–1783, Sep. 2016.
[38] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[39] E. Bjornson, M. Matthaiou, and M. Debbah, "A new look at dual-hop relaying: Performance limits with hardware impairments," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4512–4525, Nov. 2013.
[40] S. M. Moser, "Expectations of a noncentral chi-square distribution with application to IID MIMO Gaussian fading," in *Proc. IEEE ISIT*, Dec. 2008, pp. 1–6.

**MILAD TATAR MAMAGHANI** received the B.Sc. degrees in electrical engineering and communications and control from the Amirkabir University of Technology, Tehran, Iran. He is currently pursuing the master's degree (by Research) in telecommunications engineering with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, Australia. His research interests include wireless communications and networking, physical-layer security, and UAV communications. He has served as a Reviewer for some prestigious IEEE Transactions and the IET journals.

**YI HONG** (S'00–M'05–SM'10) received the Ph.D. degree in electrical engineering and telecommunications from the University of New South Wales (UNSW), Sydney. She is currently a Senior Lecturer with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, Australia. Her research interests include communication theory and coding and information theory with applications to telecommunication engineering. She received the NICTA-ACoRN Earlier Career Researcher Award at the Australian Communication Theory Workshop, Adelaide, Australia, in 2007. She currently serves on the Australian Research Council College of Experts in the period of 2018 to 2020. She was a Technical Program Committee Member for many IEEE leading conferences. She was the Publicity Chair of the IEEE Information Theory Workshop, Sicily, in 2009, the Technical Program Committee Chair of the Australian Communications Theory Workshop, Melbourne, in 2011, and the General Co-Chair of the IEEE Information Theory Workshop, Hobart, in 2014. She was an Associate Editor of the IEEE WIRELESS COMMUNICATION LETTERS and the TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES (ETT).