Enabling Secure UAV-Assisted IoT Communications with RF Energy Harvesting in the Presence of Eavesdropper

Gaurav K. Pandey[†], Devendra Singh Gurjar[†], Suneel Yadav[‡], Dragana Krstic[§], and Yuming Jiang[¶]
[†]National Institute of Technology Silchar, India, Email: {gaurav_rs, dsgurjar}@ece.nits.ac.in
[‡]Indian Institute of Information Technology Allahabad, India, Email: suneel@iiita.ac.in
[§]University of Nis, Faculty of Electronic Engineering, Serbia, Email: dragana.krstic@elfak.ni.ac.rs
[¶]Norwegian University of Science and Technology (NTNU), Norway, Email: yuming.jiang@ntnu.no

***Abstract*—This paper considers multiple unmanned aerial vehicles (UAVs) to enable secure and reliable communications between energy-constrained Internet of Things devices (IoDs). First, these IoDs harvest energy using the radio frequency (RF) signals transmitted from a power beacon. Then, the harvested energy is used to exchange information via multiple UAV relays in the presence of an eavesdropper. Among multiple UAVs, the best UAV relay is selected based on the achievable signal-to-noise ratio of the first hop. The selected UAV applies a decode-and-forward (DF) operation to forward the information. However, an eavesdropper present in the vicinity of IoDs can wiretap the information transmission through the UAV-to-ground channel. Thus, the UAV employs artificial noise (AN) injection technique to prevent the eavesdropper from intruding on the information transmission. For modeling the composite fading channel, we use the log-normal distribution to characterize the shadowing components. Further, we adopt the Gauss-Hermite quadrature method to derive the closed-form secrecy outage probability (SOP) expression. Moreover, we offer a reliability and security trade-off analysis by providing closed-form expressions for the outage probability (OP) and intercept probability (IP) as reliability and security performance measures, respectively. The numerical and simulation results corroborate the analytical findings, highlight the impact of various channel/system parameters on the secrecy and reliability performance, and provide valuable insights into the system's behavior.**

***Index Terms*—Unmanned aerial vehicles (UAVs), wireless power transfer, artificial noise, secrecy and reliability trade-off.**

I. Introduction

The rapid advancements of Internet of Things (IoT) technology are driven by the emergence of compact, intelligent, and widely distributed sensing equipment, integrating the physical and virtual realms. However, these IoT devices (IoDs) are often deployed in remote and difficult environments, such as border areas, in the aftermath of natural or artificial disasters, etc. [1]. These conditions pose significant challenges to data acquisition and dissemination, compounded by the limited energy resources of battery-powered nanoscale IoDs, which restrict their operational lifespan. To address this issue, many energy harvesting (EH) alternatives have emerged as promising solutions for extending the functionality of IoDs [2]. Among these alternatives, radio frequency (RF) EH techniques have gained popularity due to their resilience to environmental factors compared to traditional energy harvesting sources.

On the other hand, unmanned aerial vehicles (UAVs) can offer versatile solutions for establishing on-demand infrastructure-less wireless networks in various applications, including search and rescue missions, disaster response, and military operations [3]. Moreover, UAVs leverage line-of-sight (LoS) air-to-ground (A2G) or ground-to-air (G2A) channels, making them particularly suitable for scenarios where terrestrial networks are overloaded or inaccessible [4]. In such cases, UAVs can serve as aerial nodes to collect data from energy-constrained IoDs and relay it to the intended destination [5]. However, UAV links are also susceptible to shadowing effects caused by the UAV's airframe or tall obstacles [6]. Additionally, the performance of UAV-assisted networks can be impacted by hardware imperfections associated with RF transceivers, making it essential to consider these hardware impairments (HIs) for accurate performance assessment [5].

In addition to the limited operational lifespan, ensuring data security is a critical challenge in IoD communications [7]. Further, wireless channels' broadcast nature and the presence of potential eavesdroppers in unpredictable locations pose security risks to IoD links. As a result, the A2G link in UAV-assisted IoD networks may increase the likelihood of eavesdropping on transmitted data [8]. To address this concern, UAVs employ various physical layer security techniques, such as path planning, relay selection, artificial noise (AN) insertion, and cooperative jamming, to enhance the security of UAV-assisted communications [4]. For instance, the authors in [9] have focused on enhancing the covertness of full-duplex UAV relay-assisted networks by leveraging the flexible deployment capabilities of UAVs. They proposed strategies considering the presence of no-fly zones in UAV path planning and the existence of multiple eavesdroppers. Addressing the average minimum secrecy rate maximization problem, the authors in [10] have aimed to optimize the secrecy rate while accounting for the presence of multiple eavesdroppers. Further, the authors in [11] have investigated a mobile UAV-relay node that facilitates data transfer between two terrestrial users in the presence of a terrestrial eavesdropper.

The authors in [12] aimed to maximize the secrecy rate by employing AN generated by a UAV. They split the UAV's transmit power into two streams, one for serving terrestrial users and the other for emitting AN to counter eavesdropping. Exploring the problem of average secrecy rate maximization, the researchers in [13] considered a UAV emitting AN to deceive an eavesdropper while a terrestrial BS provided communication services to the users. The authors in [14] formulated a problem to maximize the worst-case secrecy rate, considering the imperfect location of an eavesdropper. They proposed a UAV serving a mobile user while jamming the eavesdropper. Focusing on the security-reliability tradeoff (SRT) in a SWIPT-based relay network, the authors in [15] introduced a friendly jammer to enhance security against eavesdroppers.

Motivated by the previous works, we aim to establish a reliable and secure multi-UAV relay system for energy-constrained IoDs in scenarios where the direct links between IoDs are heavily obstructed or shadowed. Different from [9], [10], [12]–[14], where the authors have focused only on data secrecy, we emphasize on reliability-security aspects of the proposed system. Here, the IoDs harvest energy from the RF signals transmitted by the nearby power beacon. Then, one of the IoDs (IoD_1) utilizes the harvested energy to transmit information to other IoD (IoD_2) with relaying assistance from multiple UAVs. We employ the SNR-based relay-selection technique to determine the best UAV for relay cooperation. Additionally, we assume the presence of a terrestrial eavesdropper capable of compromising the secrecy of the transmitted information through the A2G link. Unlike [11], [15], where the authors have utilized a separate UAV jammer to counter the eavesdropping, we employ the same UAV that performs both relaying and AN injection. Thus, during the second phase, the selected UAV decodes the signal, introduces self-generated AN, and broadcasts it to the intended node. The system experiences composite channel fading conditions that include log-normal distribution for shadowing and Nakagami-m distribution for small-scale fading, owing to the prevalence of the UAV's A2G link. We derive closed-form expressions for the secrecy outage probability (SOP), outage probability (OP), and intercept probability (IP). We offer valuable insights into the secrecy and reliability-security aspects of the proposed work through extensive numerical analysis.

Notations: The probability, PDF and CDF of a random variable X are denoted by $\Pr[\cdot]$, $f_X(\cdot)$, and $F_X(\cdot)$, respectively. $\Gamma(\cdot)$, $\Gamma(\cdot,\cdot)$ and $\Upsilon(\cdot,\cdot)$ are the complete, upper and lower incomplete gamma functions. $\mathcal{K}_v(\cdot)$ represents modified Bessel function of second kind of vth order.

II. System Model Discussion

A. System Model

We consider multiple UAV relays-assisted secure communication between energy-constrained IoDs in the presence of an eavesdropper, as illustrated in Fig. 1. There can be many IoDs deployed in a small geographical region, however, we focus on accomplishing information dissemination between a selected pair of IoDs. All the involved nodes, i.e., a power beacon (B), N number of UAVs (U_n) for $n \in \{1, \cdots, N\}$, the IoDs pair (IoD$_1$ and IoD$_2$), and an eavesdropper (Eve), are assumed to be equipped with single antenna devices and operate in half-duplex mode. The horizontal distances between the involved entities are taken as $r_{i,j}$ for $(i,j) \in \{(b,1);(1,n);(n,2);(n,e)\}$ with subscripts b, 1, 2, n, and e indicate the nodes B, IoD$_1$, IoD$_2$, U_n, and Eve, respectively. Thereby, the distances between these nodes and the elevation angles are calculated as $d_{i,j} = \sqrt{h^2+r_{i,j}^2}$ and $\theta_i = \arctan\left(h/r_{i,j}\right)$, respectively, where h is the height of the U_n. The data transmission block of duration T is divided into three phases, i.e., the wireless power transfer (WPT) phase, and two information transmission (IT) phases, as depicted in Fig. 2.

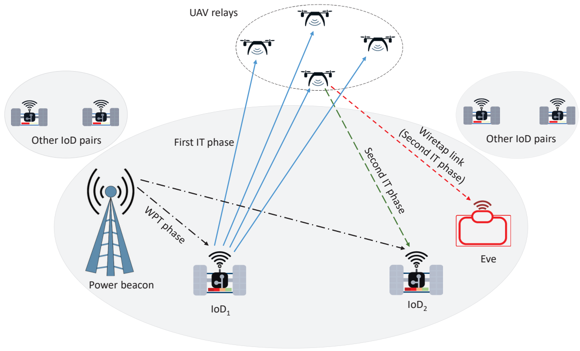

Fig. 1. UAV-enabled secure IoD communications.

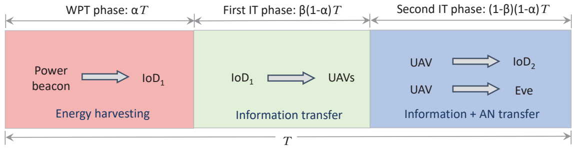

Fig. 2. Transmission block for the considered system.

Here, the main objective is to enable information transfer between IoD$_1$ and IoD$_2$, where the direct path is heavily obstructed. To achieve this, we utilize a multiple UAV-assisted relaying scheme. The RF transmission from a nearby located B is leveraged for energy harvesting at IoD$_1$ in the WPT phase, i.e., αT, where α refers to the TS factor, satisfying $0 < \alpha < 1$. Thereafter, IoD$_1$ transmits the information to the multiple UAVs in the first IT phase, i.e., $\beta(1-\alpha)T$. The UAV corresponding to best instantaneous SNR is selected for relaying the information to IoD$_2$ by applying decode-and-forward (DF) operation. We assume that a terrestrial Eve is located in the vicinity of IoD$_2$, which can wiretap the information through A2G channel. Thus, in the second IT phase, the selected UAV adds self-generated AN to increase the security of data before transmitting it to IoD$_2$.

B. Channel Model

We assume block fading scenario and adopt a composite channel model that combines Nakagami-m distribution for small-scale fading and a log-normal distribution for capturing the effects of shadowing for the channels between UAV to ground nodes. For example, the PDF of a composite fading channel X can be derived using the Gauss-Hermite Quadrature technique [16] and is given as

$$f_X(x) = \frac{1}{\sqrt{\pi}} \sum_{n=1}^{N} w_n \left(\frac{m_{i,j}}{\mathcal{A}_{i,j}}\right)^{m_{i,j}} \frac{x^{m_{i,j}-1}}{\Gamma[m_{i,j}]} e^{-\left(\frac{m_{i,j}x}{\mathcal{A}_{i,j}}\right)}, \quad (1)$$

where $\mathcal{A}_{i,j} = 10^{\left(\sqrt{2}\delta_{i,j}t_n + \vartheta_{i,j}\right)/10}$ and $m_{i,j}$ is the fading severity parameter for the channel between the nodes i and j. Gauss-Hermite quadrature weights are given by w_n and Hermite polynomial roots are given by $[t_n]_{n=1}^{N}$ with N samples. $\delta_{i,j} = c_1 \mathrm{e}^{-\theta_{i,j}d_1}$ represents the standard deviation for the environment parameters c_1 and d_1. $\vartheta_{i,j}$ denotes the average path loss between the links [16], which is evaluated based on LoS and NLoS probabilities, and $\vartheta_{i,j}$ is mathematically given as $\vartheta_{i,j} = (\mathcal{P}_{\mathrm{LOS}}(\theta) \times \vartheta_{\mathrm{LoS}} + \mathcal{P}_{\mathrm{NLoS}}(\theta) \times \vartheta_{\mathrm{NLoS}})$, where $\mathcal{P}_{\mathrm{LoS}}$ and $\mathcal{P}_{\mathrm{NLoS}}$ represent the LoS and NLoS probabilities, respectively. Here, $\mathcal{P}_{\mathrm{LoS}}(\theta) = 1/(1 + a\mathrm{e}^{-b(\theta_{i,j}-a)})$, and $\mathcal{P}_{\mathrm{NLoS}}(\theta) = (1 - \mathcal{P}_{\mathrm{LoS}}(\theta))$, a and b are environment-dependent parameters, and θ denotes the angle between terrestrial nodes and UAV relay. Additionally, mean path-loss for LoS and NLoS components is given as ϑ_{LoS} and $\vartheta_{\mathrm{NLoS}}$, respectively, and are expressed as $\vartheta_{\mathrm{LoS}} = 20\log_{10}(4\pi f_c/c) + 20\log_{10} d_{i,j} + \psi_{\mathrm{LoS}}$, and $\vartheta_{\mathrm{NLoS}} = 20\log_{10}(4\pi f_c/c) + 20\log_{10} d_{i,j} + \psi_{\mathrm{NLoS}}$, where c and f_c denotes the speed of light and carrier frequency, ψ_{LoS}, and ψ_{NLoS} are the propagation environment constants [6].

On taking the HIs into account, the received signal is given as $y_{i,j} = h_{i,j}(\sqrt{P}x_i + \zeta_{i,j}) + n_{i,j}$, where $\zeta_{i,j} \sim \mathcal{CN}(0, k^2P)$ represents the distortion noise resulting from the transceiver impairments, P denotes the transmit power, and $k = \sqrt{k_i^2 + k_j^2}$ with k_i and k_j indicating the impairment levels of the transmitter and receiver, respectively [17]. The special case where $\zeta_{i,j} = 0$ corresponds to the ideal case.

C. Signal-to-Noise-plus-Distortion-Ratios (SNDRs)

In the WPT phase, IoD_1 harvests the energy from the RF signal transmitted by B, which is given by $\mathcal{E}_H = \eta(P_b|h_{b,1}|^2)\alpha T$, where P_b is the transmit power of B, η is the energy conversion efficiency, and $h_{b,1}$ is the channel coefficient. Thus, the power available at the IoD_1 is given by $P_1 = \frac{\eta\alpha(P_b|h_{b,1}|^2)}{\beta(1-\alpha)}$. In the first IT phase, i.e., the signal received at the $\mathsf{U_n}$ node from IoD_1 in the presence of HIs can be given as $y_{1,n} = (\sqrt{P_1}x_1 + \zeta_{1,n})h_{1,n} + n_u$, where P_1 and x_1 are the transmit power and unit energy symbol transmitted by IoD_1, respectively and $n_u \sim \mathcal{CN}(0, N_0)$ represents the additive white Gaussian noise (AWGN) at $\mathsf{U_n}$. Thus, based on the received signal, the SNDR at the $\mathsf{U_n}$ can be expressed as

$$\gamma_{1,n} = \frac{\eta\alpha P_b|h_{b,1}|^2|h_{1,n}|^2}{\eta\alpha k^2 P_b|h_{b,1}|^2|h_{1,n}|^2 + \beta(1-\alpha)N_0}. \quad (2)$$

From the multiple UAV relays, the best IoD_1-$\mathsf{U_n}$ relay link is selected by using the SNR-based relay selection technique in the first IT phase [18]. This is mathematically given as

$$n^* = \arg \max_{n \in \{1,\cdots,N\}} \{\gamma_{1,n}\}. \quad (3)$$

Next, in the second IT phase, the selected UAV decodes the information signal received from the IoD_1 [12], [19]. Then, it adds the self-generated AN with the signal and broadcasts it so that the Eve should be unable to access the confidential information [20]. Thus, the signals received at IoD_2 and Eve are given as

$$y_{n^*,l} = \Big(\underbrace{\sqrt{\epsilon P_{n^*}}x_{n^*}}_{\text{Information signal}} + \underbrace{\sqrt{(1-\epsilon)\,P_{n^*}}\,x_{\mathrm{A}}}_{\text{AN}} + \zeta_{n^*,l}\Big)h_{n^*,l} + n_l, \quad (4)$$

where $l \in \{2, e\}$, x_{n^*} and P_{n^*} are the unit energy symbol and transmit power at $\mathsf{U_{n^*}}$, $x_{\mathrm{A}} \in \mathcal{CN}(0,1)$ is the normalized complex Gaussian AN transmitted by $\mathsf{U_{n^*}}$, $n_l \sim \mathcal{CN}(0, N_0)$ represents the AWGN at IoD_2 and Eve, and $0 < \epsilon < 1$ is the power allocation factor for deciding the power dedicated to information signal and AN. It is important to note that the AN can be eliminated by the IoD_2 node, but the Eve fails to remove the AN from the received signal [12], [21]. Thus, based on the signal received in (4), the instantaneous SNDRs at the IoD_2 and Eve can be expressed, respectively, as

$$\gamma_{n,2} = \frac{\epsilon P_n|h_{n,2}|^2}{\epsilon k^2 P_n|h_{n,2}|^2 + N_0}, \quad (5)$$

$$\gamma_{n,e} = \frac{\epsilon P_n|h_{n,e}|^2}{(1 - \epsilon + k^2)P_n|h_{n,e}|^2 + N_0}. \quad (6)$$

III. Performance Analysis

A. Secrecy Outage Probability (SOP)

We define the SOP as an event that occurs when the secrecy capacity $\mathcal{C}_{\mathrm{s}}$, which is defined as the difference between the instantaneous capacity of a legitimate link and eavesdropper's link, falls below the target secrecy rate, $\mathcal{R}_{\mathrm{th}}$ (bps/Hz) [4]. The SOP is mathematically expressed as

$$\mathcal{P}_{\mathrm{sop}} = \Pr[\mathcal{C}_{\mathrm{s}} < \mathcal{R}_{\mathrm{th}}] = \Pr\left[\frac{1+\gamma_{n,2}}{1+\gamma_{n,e}} < \phi\right] \simeq \Pr\left[\frac{\gamma_{n,2}}{\gamma_{n,e}} < \phi\right], \quad (7)$$

where $\mathcal{C}_{\mathrm{s}} = (\mathcal{C}_{n,2} - \mathcal{C}_{n,e})$ for $\mathcal{C}_{n,2} = (1-\beta)(1-\alpha)\log_2(1+\gamma_{n,2})$ and $\mathcal{C}_{n,e} = (1-\beta)(1-\alpha)\log_2(1+\gamma_{n,e})$, and $\phi = 2^{\mathcal{R}_{\mathrm{th}}/(1-\beta)(1-\alpha)}$. We derive the expression for SOP in the following lemma.

Lemma 1: The expression of $\mathcal{P}_{\mathrm{sop}}$ is expressed as

$$\begin{aligned}
\mathcal{P}_{\mathrm{sop}} = {} & \frac{1}{\sqrt{\pi}} \sum_{j=0}^{J} \frac{w_j}{\Gamma[m_{n,e}]} \Upsilon\left[m_{n,e}, \frac{m_{n,e}}{A_4\mathcal{A}_{n,e}}\right] + \frac{1}{\pi} \sum_{j=0}^{J} \sum_{l=0}^{L} \frac{w_j w_l}{\Gamma[m_{n,e}]} \\
& \times \Bigg[\Gamma\left(m_{n,e}, \frac{m_{n,e}}{A_4\mathcal{A}_{n,e}}\right) - \left(\frac{m_{n,e}}{\mathcal{A}_{n,e}}\right)^{m_{n,e}} \sum_{p=0}^{m_{n,2}-1} \frac{(-1)^p}{p!} \\
& \times \left(\frac{m_{n,2}}{\mathcal{A}_{n,2}}\right)^p \left(\frac{1}{A_4}\right)^{m_{n,e}+p} e^{-\left(\frac{1}{A_4}\left(\frac{m_{n,e}}{\mathcal{A}_{n,e}} - \frac{m_{n,2}\phi}{\mathcal{A}_{n,2}}\right)\right)} \\
& \times \sum_{r=0}^{m_{n,e}+p-1} \binom{m_{n,e}+p-1}{r} \left(\frac{m_{n,e}}{\mathcal{A}_{n,e}} \frac{m_{n,2}}{\mathcal{A}_{n,e}\phi}\right)^{\frac{m_{n,2}-r}{2}} \\
& \times \mathcal{K}_{m_{n,2}-r}\left(2\sqrt{\frac{m_{n,e}}{\mathcal{A}_{n,e}} \frac{m_{n,2}}{\mathcal{A}_{n,2}} \frac{\phi}{(A_4)^2}}\right)\Bigg]. \quad (8)
\end{aligned}$$

Proof 1: Please see Appendix A.

B. Security and Reliability Trade-off (SRT) Analysis

In this section, we perform the SRT analysis for the considered system, where IP and OP are used to evaluate security and reliability performance, respectively [15], [19], [22].

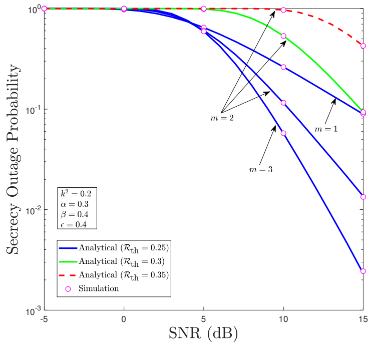

Fig. 3. SOP vs. SNR with different $\mathcal{R}_{\text{th}}$ and m.

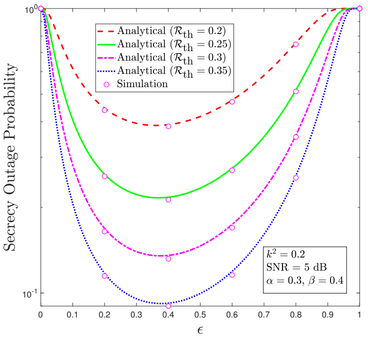

Fig. 4. SOP vs. ϵ with different $\mathcal{R}_{\text{th}}$.

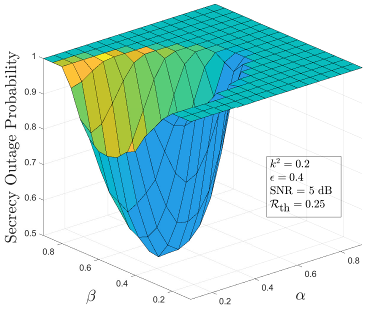

Fig. 5. SOP vs. α and β.

1) Outage Probability (OP): The system is said to be in outage when the instantaneous data rate falls below the pre-defined target rate, $\mathcal{R}_{\text{th}}$. The OP is given as

$$\begin{aligned}\mathcal{P}_{\text{out}} &= 1-(1-\Pr[\mathcal{R}_{1,n^*}<\mathcal{R}_{\text{th}}])(1-\Pr[\mathcal{R}_{n,2}<\mathcal{R}_{\text{th}}])\\ &= 1-(1-\Pr[\gamma_{1,}<\psi])(1-\Pr[\gamma_{n,2}<\delta]), \qquad (9)\end{aligned}$$

where $\mathcal{P}_{1,n^*}=\Pr[\mathcal{R}_{1,n^*}<\mathcal{R}_{\text{th}}]$ and $\mathcal{P}_{n,2}=\Pr[\mathcal{R}_{n,2}<\mathcal{R}_{\text{th}}]$ are terms corresponding decoding of signal in the first and second IT phases, $\mathcal{R}_{1,n^*}=\beta(1-\alpha)\log_2(1+\gamma_{1,n^*})$ and $\mathcal{R}_{n,2}=(1-\beta)(1-\alpha)\log_2(1+\gamma_{n,2})$, $\psi=2^{\mathcal{R}_{\text{th}}/\beta(1-\alpha)}-1$ and $\delta=2^{\mathcal{R}_{\text{th}}/(1-\beta)(1-\alpha)}-1$ are the target SNRs of different links, respectively. Using (3) and (9), the expression for the OP can be expressed as

$$\begin{aligned}\mathcal{P}_{\text{out}} &= 1-\left(1-\prod_{n=1}^{N}\Pr\left[\gamma_{1,n}<\psi\right]\right)(1-\Pr[\gamma_{n,2}<\delta])\\ &= 1-(1-(F_{\gamma_{1,n}}(\psi))^{N})(1-F_{\gamma_{n,2}}(\delta)). \qquad (10)\end{aligned}$$

We provide the expression of $F_{\gamma_{1,n}}(\psi)$ in the following lemma.

Lemma 2: The expression of $F_{\gamma_{1,n}}(\psi)$ is expressed as

$$\begin{aligned}F_{\gamma_{1,n}}(\psi) = &\frac{1}{\sqrt{\pi}}\sum_{q=0}^{Q}w_q\left[1-\frac{1}{\Gamma[m_{1,n}]}\sum_{i=0}^{m_{b,1}-1}\frac{(-1)^i}{i!}\left(\frac{m_{1,n}}{\mathcal{A}_{1,n}}\right)^{m_{1,n}}\right.\\ &\times\left(\frac{m_{b,1}B_3\psi}{\mathcal{A}_{b,1}(B_1-\psi B_2)}\right)^{i}\left(\frac{m_{b,1}\mathcal{A}_{1,n}B_3\psi}{\mathcal{A}_{b,1}m_{1,n}(B_1-\psi B_2)}\right)^{\frac{m_{1,n}-i}{2}}\\ &\left.\times\, 2\mathcal{K}_{m_{1,n}-i}\left(2\sqrt{\frac{m_{b,1}}{\mathcal{A}_{b,1}}\frac{m_{1,n}}{\mathcal{A}_{1,n}}\frac{B_3\psi}{(B_1-\psi B_2)}}\right)\right]. \qquad (11)\end{aligned}$$

Proof 2: Please see Appendix B.

On utilizing (5) and then performing some mathematical simplifications, we can express $F_{\gamma_{n,2}}(\delta)=\Pr[|h_{n,2}|^2<\Theta]$, where $\Theta=\left(\frac{\delta}{A_1-A_2\delta}\right)$. Similar to (1), the PDF of $|h_{n,2}|^2$ can be obtained and substituted in the expression of CDF $F_{\gamma_{n,2}}(\delta)=\int_0^{\Theta}f_{|h_{n,2}|^2}(\delta)dz$. We can obtain the CDF of $F_{\gamma_{n,2}}(\delta)$ by the aid of [23, eq. (3.381.1)] as

$$F_{\gamma_{n,2}}(\delta)=\frac{1}{\sqrt{\pi}}\sum_{c=0}^{C}\frac{w_c}{\Gamma[m_{n,2}]}\Upsilon\left[m_{n,2},\Theta\frac{m_{n,2}}{\mathcal{A}_{n,2}}\right]. \qquad (12)$$

2) Intercept Probability (IP): An intercept event is encountered when the eavesdropper's capacity becomes higher than the pre-defined target rate [15], [19]. This is mathematically given as

$$\mathcal{P}_{\text{int}}=\Pr[\mathcal{C}_{n,e}>\mathcal{R}_{\text{th}}]=1-F_{\gamma_{n,e}}(\varphi). \qquad (13)$$

We can obtain $F_{\gamma_{n,e}}(\varphi)=\Pr[|h_{n,e}|^2<\Xi]$ by using (6), where $\Xi=\left(\frac{\varphi}{A_1-A_3\varphi}\right)$. Followed by performing necessary simplifications as done to acquire (12), we can obtain the CDF of $F_{\gamma_{n,e}}(\varphi)$ by the aid of [23, eq. (3.381.1)] as

$$F_{\gamma_{n,e}}(\varphi)=\frac{1}{\sqrt{\pi}}\sum_{g=0}^{G}\frac{w_g}{\Gamma[m_{n,e}]}\Upsilon\left[m_{n,e},\Xi\frac{m_{n,e}}{\mathcal{A}_{n,e}}\right], \qquad (14)$$

where $\mathcal{A}_{n,e}=10^{\left(\sqrt{2}\delta_{n,e}t_g+\mu_{n,e}\right)/10}$ and w_g provides the weights of the Gauss-Hermite quadrature.

IV. Numerical Results

In this section, we provide the numerical and simulation results for SOP and SRT analysis and verify the accuracy of the analytical formulations. Throughout this section, $P_b=P_n=P$ and P/N_0 represents the transmit SNR. Gauss-Hermite quadrature approximation coefficients are taken as $J=L=G=Q=C=15$. The UAV's operational height, $h=30$ m, and $r_{i,j}=50$ m for $(i,j)\in\{(b,1);(1,n);(n,2)\}$ and $r_{n,e}=60$ m and $f_c=700$ MHz. For the sake of simplicity, the fading severity parameter, $m_{i,j}=m=2$. We consider a dense urban environment scenario with the following parameters: $a=12.081$, $b=0.1139$, $(c_1,d_1)=(9.64,0.04)$, $(c_2,d_2)=(30.83,0.04)$, $(\psi_{\text{LoS}},\psi_{\text{NLoS}})=(1,20)$. The Monte-Carlo simulations are performed for 10^5 iterations to acquire accurate results.

Fig. 3 illustrates the SOP performance for varying transmit SNR with different values of $\mathcal{R}$th and m. It can be observed from the curves that the SOP at IoD2 decreases with an increase in transmit SNR for the fixed $\mathcal{R}_{\text{th}}$ value. However, the SOP performance degrades with an increase in $\mathcal{R}_{\text{th}}$. This trend is expected as the instantaneous achievable secrecy rate corresponding to the transmit SNR tends to fall below the increasing value of target secrecy rate. Additionally, it can be

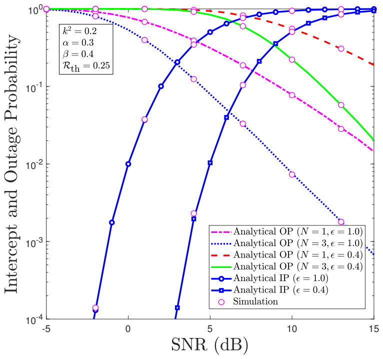

Fig. 6. IP and OP vs. transmit SNR for different values of N and ϵ.

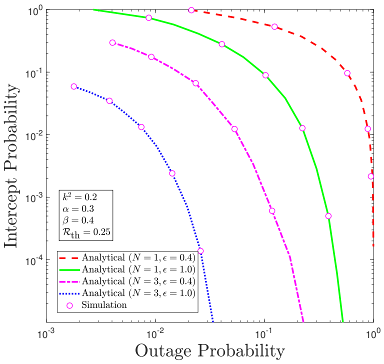

Fig. 7. Analyzing SRT with IP vs. OP curves.

observed that increasing the value of $m \in \{1, 2, 3\}$ improves the SOP performance.

Fig. 4 displays the SOP versus ϵ curves for different values of $\mathcal{R}_{\text{th}}$. From the obtained curves, it can be inferred that the SOP is minimum in the mid-range of ϵ, while it drastically increases for lower and higher values of ϵ. When ϵ is too low, the power allocated for IT decreases, leading to increased SOP. On the other hand, for higher ϵ values, the power allocated to AN decreases, resulting in degraded SOP performance. Thus, it can be concluded that the minimum SOP can be achieved for an optimal value of ϵ using the curves provided in Fig. 4. The SOP performance corresponding to different α and β values are depicted in the 3D plot shown in Fig. 5. As the time allocation for WPT and overall information transfer between the IoDs are realized by α and β, illuminating the combined impact of these parameters on the system's performance and finding the optimal values of these parameters for achieving desired system performance are of particular relevance. The convex nature of the SOP plot suggests that there is an optimal combination of α and β, i.e., $\alpha = 0.3$ and $\beta = 0.5$ at which minimum SOP can be obtained.

Figs. 6 and 7 offer valuable insights into the trade-off between security and reliability of the system. Further, $\epsilon = 1$ corresponds to the conventional information transmission scenario, where no AN is injected by the UAV. In Fig. 6, the plot illustrates the IP and OP as a function of transmit SNR for different values of N and ϵ. As the transmit SNR increases, both the OP with both single-UAV and multiple-UAVs cases decrease. Notably, the outage performance improves significantly with the increasing number of UAV relays. This is due to the fact that with more number of UAV relays, system can achieve better diversity order resulting in improved OP performance.

Further, from Fig. 6, it can be observed that the IP increases as the transmit SNR increases, which is expected since a higher transmit SNR improves the wiretap channel's capacity. It is shown that with $\epsilon = 1$, the IP performance is poor than that for $\epsilon = 0.4$. This implies the existence of a trade-off between security and reliability during information transmission in the presence of an eavesdropper. Fig. 7 provides IP versus OP curves for different values of ϵ and N. It demonstrates that the SRT performance can be concurrently improved by increasing the number of UAVs in the network. Therefore, it can be concluded that multi-UAV relaying can significantly enhance outage performance, while the AN injection scheme can greatly improve data secrecy against eavesdroppers. This results in a trade-off between security and reliability of the considered system.

V. Conclusion

This paper focused on establishing a reliable relay link between the energy-constrained IoD pair and improving the secrecy in the information transmission. We investigated the security and reliability performance of multiple UAVs-assisted and WPT-enabled IoDs whose direct link is heavily shadowed. Here, we utilized SNR-based relay selection and AN injection to enhance the reliability and secrecy of the transmitted information, respectively. By considering the HIs, we assessed the secrecy performance in terms of the SOP and SRT. We obtained the closed-form expressions of SOP, IP, and OP by considering the composite fading channel model, i.e., log-normal and Nakagami-m distributions. Through the simulation results, we demonstrated that the secrecy performance of the system is significantly affected by various factors such as SWIPT parameter, target rate, number of UAVs in the network, and power allocation for AN and IT phase.

Appendix A

On substituting the expressions of $\gamma_{n,2}$ and $\gamma_{n,e}$ obtained in (5) and (6) into (7), $\mathcal{P}_{\text{sop}}$ can be expressed as

$$\mathcal{P}_{\text{sop}} = \Pr\left[X < \frac{\phi Y}{1 - (\phi A_2 - A_3)Y}\right] = \underbrace{\int_0^{\frac{1}{\phi A_2 - A_3}} f_Y(y)dy}_{I_1}$$

$$+ \underbrace{\int_{\frac{1}{\phi A_2 - A_3}}^{\infty} f_Y(y) \int_0^{\frac{\phi y}{1-(\phi A_2 - A_3)y}} f_X(x) f_Y(y) dx dy}_{I_2}, \qquad (15)$$

where $X = |h_{n,2}|^2$ and $Y = |h_{n,e}|^2$ follow log-normal distribution for shadowing and gamma distribution for Nakagami-m faded signal amplitude distribution, whose PDF is given by (1). $A_1 = (\epsilon P_n/N_0)$, $A_2 = ((1-\epsilon)P_n/N_0)$, and $A_3 = ((1-\epsilon+k^2)P_n/N_0)$. In (15), I_1 can be evaluated by leveraging [23, eq. 3.381.1]. Then, the PDFs of X and Y are substituted in I_2, and then using [23, eqs. 3.381.3] and performing change of variables, we can obtain I_2 as

$$\begin{aligned} I_2 = &\frac{1}{\pi}\sum_{j=0}^{J}\sum_{l=0}^{L}\frac{w_j w_l}{\Gamma[m_{n,e}]}\left[\Gamma\left(m_{n,e}\,,\frac{m_{n,e}}{A_4\mathcal{A}_{n,e}}\right)-\left(\frac{m_{n,e}}{\mathcal{A}_{n,e}}\right)^{m_{n,e}}\right. \\ &\times \sum_{p=0}^{m_{n,2}-1}\frac{(-1)^p}{p!}\left(\frac{m_{n,2}}{A_4\mathcal{A}_{n,2}}\right)^p e^{-\left(\frac{1}{A_4}\left(\frac{m_{n,e}}{\mathcal{A}_{n,e}}-\frac{m_{n,2}\phi}{\mathcal{A}_{n,2}}\right)\right)} \\ &\times \left(\frac{1}{A_4}\right)^{m_{n,e}}\sum_{r=0}^{m_{n,e}+p-1}\binom{m_{n,e}+p-1}{r}\int_0^\infty t^{m_{n,2}-r-1} \\ &\times \left. e^{-\left(\left(\frac{m_{n,e}}{\mathcal{A}_{n,e}}\frac{t}{A_4}\right)+\left(\frac{m_{n,2}}{\mathcal{A}_{n,e}}\frac{\phi}{tA_4}\right)\right)}dt\right], \qquad (16) \end{aligned}$$

where $A_4 = \phi A_2 - A_3$. Finally, we can obtain the final expression of $\mathcal{P}_{\text{out}}$ by using [23, eq. 3.471.9] as shown in (8).

Appendix B

Let $Z = |h_{b,1}|^2$ follows gamma distribution and $V = |h_{1,n}|^2$ represents a composite channel gain which follows log-normal distribution for shadowing and gamma distribution for Nakagami-m faded signal amplitude distribution, whose PDF is given by (1). By using (2) and (10), the CDF $F_{\gamma_{1,n}}(\psi)$ can be given as

$$\begin{aligned} F_{\gamma_{1,n}}(\psi) &= \Pr\left[\frac{B_1 VZ}{B_2 VZ + B_3} < \psi\right] \\ &= \int_0^\infty F_Z\left(\frac{B_3\psi}{(B_1 - B_2\psi)v}\right) f_V(v)dv, \qquad (17) \end{aligned}$$

where $B_1 = \eta\alpha P_b/N_0$, $B_2 = \eta\alpha k^2 P_B/N_0$, and $B_3 = \beta(1-\alpha)$. On inserting the CDF of composite channel distribution and PDF given by (1) into (17) and then performing some mathematical simplifications using [23, eqs. (3.381.3),(3.471.9)], we can get $F_{\gamma_{1,n}}(\psi)$ as in (11).

Acknowledgement

This work was partially supported under the Mathematical Research Impact Centric Support (MATRICS) Grant by SERB-DST, Govt. of India (Grant No. MTR/2022/000035), and India–Serbia Scientific and Technological Cooperation Program between the DST, GoI, and the Ministry of Science, Technological Development and Innovation of the Republic of Serbia (Grant No. DST/ICD/Serbia/P-04/2022).

References

[1] D. Ma, G. Lan, M. Hassan, W. Hu, and S. K. Das, "Sensing, computing, and communications for energy harvesting IoTs: A survey," *IEEE Commun. Surv. & Tuts.*, vol. 22, no. 2, pp. 1222–1250, 2020.

[2] 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. Surv. & Tuts.*, vol. 20, no. 1, pp. 264–302, 2018.

[4] 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.

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

[5] M. M. Azari, G. Geraci, A. Garcia-Rodriguez, and S. Pollin, "UAV-to-UAV communications in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 9, pp. 6130–6144, 2020.

[6] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Commun. Letts.*, vol. 3, no. 6, pp. 569–572, 2014.

[7] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, C. Nguyen, D. Niyato, F. Yu, and M. Guizani, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Sur. & Tuts.*, vol. PP, 07 2021.

[8] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, pp. 12–18, 10 2019.

[9] R. Zhang, X. Chen, M. Liu, N. Zhao, X. Wang, and A. Nallanathan, "UAV relay assisted cooperative jamming for covert communications over rician fading," *IEEE Trans. Veh. Tech.*, vol. 71, no. 7, pp. 7936–7941, 2022.

[10] R. Li, Z. Wei, L. Yang, D. W. K. Ng, J. Yuan, and J. An, "Resource allocation for secure multi-UAV communication systems with multi-eavesdropper," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4490–4506, 2020.

[11] J. Miao and Z. Zheng, "Cooperative jamming for secure UAV-enabled mobile relay system," *IEEE Access*, vol. 8, pp. 48 943–48 957, 2020.

[12] K. Xu, M.-M. Zhao, Y. Cai, and L. Hanzo, "Low-complexity joint power allocation and trajectory design for UAV-enabled secure communications with power splitting," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1896–1911, 2021.

[13] Y. Wang, L. Chen, Y. Zhou, X. Liu, F. Zhou, and N. Al-Dhahir, "Resource allocation and trajectory design in UAV-assisted jamming wideband cognitive radio networks," *IEEE Trans. Cog. Commun. Net.*, vol. 7, no. 2, pp. 635–647, 2021.

[14] W. Wang, X. Li, R. Wang, K. Cumanan, W. Feng, Z. Ding, and O. A. Dobre, "Robust 3D-trajectory and time switching optimization for dual-UAV-enabled secure communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3334–3347, 2021.

[15] T. N. Nguyen, D.-H. Tran, T. V. Chien, V.-D. Phan, M. Voznak, P. T. Tin, S. Chatzinotas, D. W. K. Ng, and H. V. Poor, "Security–reliability tradeoff analysis for SWIPT- and AF-based IoT networks with friendly jammers," *IEEE Internet of Things J.*, vol. 9, no. 21, pp. 21 662–21 675, 2022.

[16] G. K. Pandey, D. S. Gurjar, S. Yadav, and S. Solanki, "UAV-empowered IoT network with hardware impairments and shadowing," *IEEE Sensors Letts.*, vol. 7, no. 7, pp. 1–4, 2023.

[17] Y. Cai, Z. Wei, R. Li, D. W. K. Ng, and J. Yuan, "Joint trajectory and resource allocation design for energy-efficient secure UAV communication systems," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4536–4553, 2020.

[18] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, 2015.

[19] J. Zhu, Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Security–reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825–5831, 2016.

[20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[21] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577–9581, 2017.

[22] Y. Zou, "Intelligent interference exploitation for heterogeneous cellular networks against eavesdropping," *IEEE J. Selected Areas Commun.*, vol. 36, no. 7, pp. 1453–1464, 2018.

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