Cooperative Friendly Jamming in Swarm UAV-assisted Communications with Wireless Energy Harvesting

Hanh Dang-Ngoc*†, Diep N. Nguyen†, Dinh Thai Hoang†, Khuong Ho-Van*, Eryk Dutkiewicz†
* Ho Chi Minh City University of Technology, VNU-HCM, Vietnam
†School of Electrical and Data Engineering, University of Technology Sydney, Australia

***Abstract*—This article proposes a cooperative friendly jamming framework for swarm unmanned aerial vehicle (UAV)-assisted amplify-and-forward (AF) relaying networks with wireless energy harvesting. In particular, we consider a swarm of hovering UAVs that relays information from a terrestrial source to a distant mobile user and simultaneously generates jamming signals to obfuscate an eavesdropper. Due to the limited energy of the UAVs, we develop a collaborative time-switching relaying protocol which allows the UAVs to collaborate to harvest wireless energy, relay information, and jam the eavesdropper. To evaluate the secrecy rate, we derive the expressions of the secrecy outage probability (SOP) in the integral form for two popular detection techniques at the eavesdropper, i.e., selection combining and maximum-ratio combining in high signal-to-noise ratio regime. Monte Carlo simulations validate the derived SOP and show that the proposed framework outperforms the conventional AF relaying system, in terms of SOP. The insights from SOP in this work can be utilized to optimize energy harvesting time, the number of UAVs in the swarm as well as their placements, to achieve the required secrecy protection level.**

***Index Terms*—ecrecy outage probability, unmanned aerial vehicle, swarm UAVs, energy harvesting, friendly jamming, relaying network.ecrecy outage probability, unmanned aerial vehicle, swarm UAVs, energy harvesting, friendly jamming, relaying network.S**

I. Introduction

Unmanned Aerial Vehicles (UAVs), thanks to their high mobility and flexibility, have great potential applications to future communications systems. In practical UAV-assisted cellular networks, UAVs can be deployed as flying relays to provide connectivity between terrestrial nodes, which are suffering from the absence of direct links.However, due to the broadcast nature of line-of-sight (LoS) dominated aerial based wireless communications, the UAVs' communication links are vulnerable to eavesdropping or jamming.

To assist and secure the system in the presence of an eavesdropper, UAV-assisted relaying systems with friendly jamming have been recently studied in [1]–[5]. In [1], a swarm of UAVs was divided into two groups of decode-and-forward relays and jammers that transmit interference to obfuscate the eavesdropper. The secrecy outage probability (SOP) was analyzed when the eavesdroppers only listen to the relay communications phase. The flying paths and locations of UAVs can also be optimized to enhance the physical layer security of wireless networks, i.e., retreating away from the eavesdroppers [3]. A relaying UAV and a jamming UAV were utilized and optimized their flight trajectory to maximize the secrecy rate of the system in [4]. The authors in [2], [3] studied a wireless information and power transfer system which employs an energy-constrained aerial node as a relay and the full-duplex destination nodes to transmit artificial noise to confuse the malicious eavesdroppers. However, using on-ground destination nodes to jam eavesdroppers as in [2], [3] might not be effective in practical cases with severe obstacles, long distance, and deep fading. Moreover, the self-interference in full-duplex radios can also have an adverse impact on signal reception/decoding at legitimate receivers.

In this work, we propose a cooperative friendly jamming framework for swarm UAV-assisted AF relaying networks with wireless energy harvesting (EH) ability. In particular, we develop a collaborative time-switching relaying (TSR) protocol which allows a swarm of hovering UAVs to harvest wireless energy, relay information from a terrestrial source to a distant mobile user, and simultaneously generate friendly jamming signals to interfere an eavesdropper whose location can be unknown. The feasibility of powering UAVs with wireless power transfer has been reported in [6], [7] (by using microwave power transfer). To conserve on-board energy, we assume that UAVs operate in the half-duplex mode in which they receive the information from the source and jam the eavesdropper in two separate phases. During these phases, the eavesdropper can intercept the information from both the source and the relay UAV using either selection combining (SC) and maximum-ratio combining (MRC) scheme. In practice, an eavesdropper is often a passive device (i.e., not emitting signal), its location and the channel state information (CSI) between it and the legitimate transmitter are often unknown. For that, we consider the case of a randomly distributed eavesdropper. The major contributions of our work are as follows.

- Propose an effective model and protocol to utilize a swarm of wireless-powered UAVs to simultaneously relay information and to jam the eavesdropper, under a practical shadowed-Rician fading model.
- Derive the expressions of the SOP in high signal-to-noise ratio (SNR) regime for two cases of SC and MRC combining techniques at the eavesdropper in the integral form.
- Conduct the Monte Carlo simulations to verify the ex-

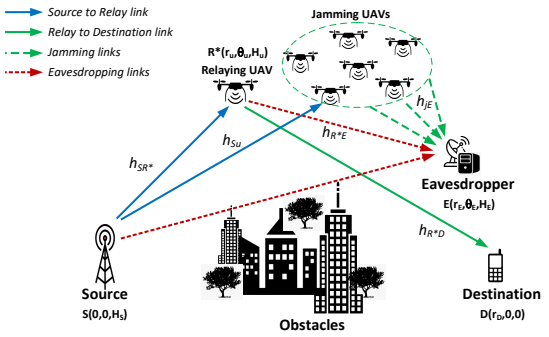


Fig. 1: System model of UAV-assisted relaying network.

pressions and obtain the engineering insights to optimize the energy harvesting time, the number of UAVs in the swarm, as well as their placements, to achieve a given secrecy protection level.

Notations: $|\cdot|$ is the Euclidean norm; $f_X(\cdot)$ and $F_X(\cdot)$ denote the probability density function (PDF) and the cumulative distribution function (CDF) of the random variable (r.v.) X, respectively; $\mathbb{E}(\cdot)$ is the statistical expectation operation; the operation $\Pr(\cdot)$ returns probability.

II. System Model

Consider a UAV-aided relaying system as depicted in Fig. 1, in which a terrestrial BS S communicates with an on-ground mobile user D, in the presence of an eavesdropper E on the ground. We assume that the direct link between S and D is not available, e.g., due to blockages and/or long distance. For that, the communications and security of the transmission from S to D are assisted by a swarm of U UAVs that function as a relay and friendly jammers. Let R_u denote the u-th UAV where $u \in \Phi_u = \{1, 2, ..., U\}$. Due to their limited energy, we assume that UAVs are only equipped with a single antenna, operate in the half-duplex AF mode, and can wirelessly harvest power from S [8]. Specifically, the TSR protocol between S and D is accomplished over three phases with the total length of T, i.e., the EH phase, the transmission from S to the UAVs phase, and the AF from the relay UAV to D phase. Here, we adopt the two equal time-slots AF relaying system [2]. During the EH phase of length αT, $\alpha \in [0, 1]$ where α is the EH time factor, all U UAVs scavenge RF energy from S. In the second phase of length $(1-\alpha)T/2$, S broadcasts the information signal to all the UAVs, and is susceptible to eavesdropping by E. Note that in the second phase, all half-duplex UAVs that are in the reception mode (to receive the signal from S) cannot harvest energy and jam E. Then, in the third phase of length $(1-\alpha)T/2$, the UAV R^* with the highest SNR over S-to-UAVs links uses the harvested energy to AF the received signals to D, while $(U-1)$ other UAVs R_j (with $j \in \Phi_u \backslash R^*$) use their harvested energy to jam E. In order to eliminate the burden of signal synchronization among UAVs, we consider that only one UAV is selected as a relay to forward signals to D. Note that the friendly jamming signals can be completely canceled at D, e.g., using the successive cancellation or projection technique [5].

All the channels are assumed to be quasi-static, i.e., unchanged during each transmission time slot T but independently vary from one time slot to another [9]. The channel coefficient between nodes u and v is denoted as h_{uv}, which has the corresponding channel gain $|h_{uv}|^2$. Specifically, h_{Su}, h_{SR^*} and h_{SE} are the channel coefficient between S and the u-th UAV, R^* or E, respectively. The channel coefficients between R^* and D, R^* and E, the j-th jamming UAV and E are h_{R^*D}, h_{R^*E} and h_{jE}, respectively. Due to the strong LoS components, all the channels between UAVs and ground nodes are modeled by shadowed-Rician fading[1] with the PDF given by

$$f_{|h_{uv}|^2}(x) = \mathcal{A}e^{-\mathcal{B}x}{}_1F_1(m_S; 1; \vartheta x), x \geq 0, \quad (1)$$

where $\mathcal{A} = (2bm_S/(2bm_S + \Omega))^{m_S}/2b$, $\mathcal{B} = 1/2b$, $\vartheta = \Omega/(2bm_S + \Omega)/2b$ with Ω and $2b$ being the average power of LoS and multipath components, respectively, m_S is the fading severity parameter, and ${}_1F_1(\cdot;\cdot;\cdot)$ is the confluent hypergeometric function of the first kind [11]. For any arbitrary fading severity parameter m_S, one can simplify ${}_1F_1(m_S; 1; \vartheta x)$ to obtain the PDF and CDF as [12]

$$f_{|h_{uv}|^2}(x) = \sum_{l=0}^{m_S-1} \zeta_{uv} x^l e^{-\eta_{uv}x}, \quad (2)$$

$$F_{|h_{uv}|^2}(x) = 1 - \sum_{l=0}^{m_S-1} \sum_{q=0}^{l} \kappa_{uv} x^q e^{-\eta_{uv}x}, \quad (3)$$

where $\zeta_{uv} = \mathcal{A}(m_S - l)_l(\vartheta)^l/(l!)^2$, $\kappa_{uv} = \zeta_{uv}(l!/q!)\eta_{uv}^{-(l+1-q)}$, and $\eta_{uv} = \mathcal{B} - \vartheta$, in which $(m_S - l)_l = \Gamma(m_S)/\Gamma(m_S - l)$ is the Pochhammer symbol [13]. We denote $X = |h_{SR^*}|^2$, $Y = |h_{R^*D}|^2$, $Z = |h_{R^*E}|^2$. Therefore, $\{\zeta_X, \kappa_X, \eta_X\}$, $\{\zeta_Y, \kappa_Y, \eta_Y\}$, and $\{\zeta_Z, \kappa_Z, \eta_Z\}$ are the corresponding channel gain of S-to-R^*, R^*-to-D, and R^*-to-E links, respectively. The terrestrial link between S and E is subject to undergo small-scale Rayleigh model due to many obstructions on ground [9] with the PDF and CDF as

$$f_W(x) = e^{-x}, \quad F_W(x) = 1 - e^{-x}, \quad (4)$$

respectively, where $W = |h_{SE}|^2$ is denoted as the channel gain of link between S and E.

We use the polar coordinate to facilitate the analysis with the coordinate origin at S, $\mathrm{p}_S = (0, 0, H_S)$, where H_S is the height of the antenna tower from the ground. UAVs are flying within a swarm whose span is very small at $\mathrm{p}_u = (r_u, \theta_u, H_u)$ to serve a mobile user D which is located at $\mathrm{p}_D = (r_D, 0, 0)$. Since the eavesdropper's location is unknown in practical applications, we consider the case that an eavesdropper E at $\mathrm{p}_E = (r_E, \theta_E, 0)$ is uniformly distributed on ground inside

[1]The shadowed-Rician distribution has been proposed to generally describe the channels between UAVs and ground nodes [10] since these channels vary significantly with UAVs' 3D locations in an area, which may be under a deep fade and shadowing.

a circular disc of radius r_c that is centered at S. The $E's$ distribution is modeled by the binomial point process Φ_E with the corresponding PDF as [14]

$$f_{\mathrm{p}_E}(r_E, \theta_E, 0) = \frac{1}{\pi {r_c}^2}, \;\; r_E \le r_c, \;\; 0 \le \theta_E \le 2\pi. \quad (5)$$

Considering the nodes' locations, the path loss at a distance d_{uv} from u to v is given by $\lambda_{uv} = \rho_0 \left(d_{uv}/d_0\right)^{-\tau}$, where τ is the path-loss exponent, and ρ_0 is the reference gain at a reference distance of d_0.The received power at v can be written as $P_v = P_u \lambda_{uv} |h_{uv}|^2$, where P_u is the transmitted power at u. The transmit power of S is P_S. The noise at all the receivers is assumed to be the Additive White Gaussian Noise following $\mathcal{CN}\left(0, \sigma^2\right)$.

A. Legitimate Communication Link

In the EH phase, following the linear EH model [15], the harvested energy at the u-th UAV is written as

$$\Xi_u = \eta \alpha T \left(P_S \lambda_{Su} |h_{Su}|^2 + \sigma^2\right), \quad (6)$$

where $0 < \eta < 1$ is the energy conversion efficiency factor which depends on the EH circuitry. In the second phase, S broadcasts its information signal to all the UAVs. The instantaneous SNR over the link between S and the u-th UAV is $\gamma_{Su} = \psi \lambda_{Su} |h_{Su}|^2$, with denotation of $\psi = P_S/\sigma^2$. At the end of this phase, only R^* is selected as a relay node according to the highest SNR criterion as $\gamma_{SR^*} = \psi \lambda_{SR^*} |h_{SR^*}|^2 = \max\limits_{u \in \Phi_u} \left(\psi \lambda_{Su} |h_{Su}|^2\right)$. The harvested energy at R^* in the EH phase is $\Xi_{R^*} = \eta \alpha T \left(P_S \lambda_{SR^*} |h_{SR^*}|^2 + \sigma^2\right)$. Then, in the third phase, R^* uses its harvested energy to AF the received signals to D with an amplification factor of

$$G_{AF} = \frac{2\Xi_{R^*}/(1-\alpha)T}{P_S \lambda_{SR^*} |h_{SR^*}|^2 + \sigma^2}. \quad (7)$$

The SNR of received signal at D is then written as

$$\gamma_D = \frac{\varepsilon \psi \lambda_{SR^*} \lambda_{R^*D} XY}{\varepsilon \lambda_{R^*D} Y + 1}, \quad (8)$$

where $\varepsilon = 2\eta\alpha/(1-\alpha)$ denotes the TSR-AF factor.

Under the assumption that the UAVs are located sufficiently apart within a swarm whose span is very small as compared to the distances from UAVs to on-ground nodes, we assume i.i.d. channels between S and UAVs with the same average received power $\lambda_{Su} = \lambda_{SR^*}$. Therefore, the UAV with the highest channel gain is selected to relay information to D. The CDF of $X = |h_{SR^*}|^2 = \max\limits_{u \in \Phi_u} |h_{Su}|^2$ is written as

$$F_X(x) = \Pr\left\{ |h_{Su}|^2 < x \,\middle|\, u \in \Phi_u \right\} = \prod_{u=1}^{U} F_{|h_{Su}|^2}(x). \quad (9)$$

Lemma 1. *The expressions for the CDF and PDF of r.v. X are presented as*

$$F_X(x) = \widetilde{\sum_u}^{U} \kappa_u x^{\chi_u} e^{-\eta_u x}, \quad (10)$$

$$f_X(x) = U \sum_{l_X=0}^{m_S-1} \zeta_X \widetilde{\sum_u}^{U-1} \kappa_u x^{l_X + \chi_u} e^{-(\eta_X + \eta_u)x}, \quad (11)$$

where

$$\widetilde{\sum_u}^{U} = \sum_{u=0}^{U} \frac{(-1)^u}{u!} \underbrace{\sum_{n_1=1}^{U} \cdots \sum_{n_u=1}^{U}}_{n_1 \neq n_2 \ldots \neq n_u} \sum_{l_1=0}^{m_S-1} \sum_{q_1=0}^{l_1} \cdots \sum_{l_u=0}^{m_S-1} \sum_{q_u=0}^{l_u},$$

$$\kappa_u = \prod_{t=1}^{u} \kappa_X, \;\; \eta_u = \sum_{t=1}^{u} \eta_X, \;\; \chi_u = q_1 + \ldots + q_u = \sum_{t=1}^{u} q_t$$

Proof. Using the multinomial theorem, the CDF of r.v. X is given as in (10). The corresponding PDF in (11) can be obtained by taking the derivative of $F_X(x)$ with respect to (w.r.t.) x to complete the proof. □

B. Eavesdropping

E is assumed to attempt to eavesdrop information in the second phase and the third phase. E can intelligently either perform SC to select the highest SNR received signal as $\gamma_E^{\mathrm{SC}} = \max\left(\gamma_{SE}, \gamma_{R^*E}^{\mathrm{J}}\right)$, or MRC with the sum SNRs as $\gamma_E^{\mathrm{MRC}} = \gamma_{SE} + \gamma_{R^*E}^{\mathrm{J}}$ to intercept the legitimate information [16].

In the second phase, E directly listens to S and receives the signal with the SNR as

$$\gamma_{SE} = \psi \lambda_{SE} W. \quad (12)$$

When all the UAVs other than the relaying one use their harvested energy to send jamming signals to E, the SNR at E over aerial links is

$$\gamma_{R^*E}^{\mathrm{J}} = \frac{\varepsilon \psi \lambda_{SR^*} \lambda_{R^*E} XZ}{\varepsilon \lambda_{R^*E} Z + 1 + P_{JE}}, \quad (13)$$

where $P_{JE} = \delta\varepsilon \sum\limits_{j=1}^{U-1} \left\{\psi \lambda_{Sj} |h_{Sj}|^2 + 1\right\} \lambda_{jE} |h_{jE}|^2$, in which δ is the factor of using harvested energy, $0 < \delta \le 1$. We assumed that all the channels between UAVs and ground nodes are i.i.d. with $\lambda_{Sj} = \lambda_{SR^*}$ and $\lambda_{jE} = \lambda_{R^*E}$, $j \in \Phi_u \backslash R^*$. The jamming power from each of the jamming UAVs can be approximated to relate to the average harvested energy from S, $P_J = \delta\varepsilon\psi\lambda_{SR^*} g$, where g is the average channel gain between S and jamming UAVs. Denote $\mathcal{J} = \sum\limits_{j=1}^{U-1} |h_{jE}|^2$, we obtain

$$\gamma_{R^*E}^{\mathrm{J}} = \frac{\varepsilon \psi \lambda_{SR^*} \lambda_{R^*E} XZ}{\varepsilon \lambda_{R^*E} Z + 1 + P_J \lambda_{R^*E} \mathcal{J}}, \quad (14)$$

Lemma 2. *The expression for the PDF of r.v. $\mathcal{J}$ is presented as*

$$f_{\mathcal{J}}(t) = \widehat{\sum_j}^{U-1} \zeta_j t^{\chi_j - 1} e^{-\eta_Z t}, \;\; U \ge 1, \quad (15)$$

where

$$\widehat{\sum_j}^{U-1} = \sum_{l_1=0}^{m_S-1} \cdots \sum_{l_{U-1}=0}^{m_S-1},$$

$$\chi_j = \sum_{j=1}^{U-1} (l_j + 1), \;\; \zeta_j = \frac{1}{(\chi_j - 1)!} \prod_{j=1}^{U-1} (\zeta_Z l_j!).$$

Proof. Using the Moment Generating Function approach, we obtain the PDF of $\mathcal{J}$ as in (15) to complete the proof. The detailed proof is omitted due to space limit. The detailed proof can be found in our technical report [17]. □

III. Secrecy Performance Analysis

Secrecy capacity is defined as the positive value of the difference between the instantaneous capacities of the legitimate and the wiretap channels. To measure the security performance of the system, the SOP is defined as the probability at which the achieved secrecy capacity of C_S is not greater than a predefined secrecy rate of C_{th}. Let $P_{out}(C_{th}) = \Pr\{C_S < C_{th}\}$ denote the SOP at C_{th}

$$P_{out}(C_{th}) = \Pr\left\{\frac{1-\alpha}{2}\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) < C_{th}\right\}, \quad (16)$$

where $\gamma_S = 2^{2\mathcal{C}_{th}/(1-\alpha)}$ denotes the target secrecy SNR. In high SNR regime, exploiting the approximation of $\frac{1+\gamma_D}{1+\gamma_E} \approx \frac{\gamma_D}{\gamma_E}$, which is adopted in literature [12], we obtain the asymptotic expression of P_{out} as

$$\bar{P}_{out}(\gamma_S) = \Pr\left\{\frac{\gamma_D}{\gamma_E} < \gamma_S\right\}. \quad (17)$$

The CSI between S and E depends on E's location via the free-space path losses, i.e., $\lambda_{SE} \propto d_{SE}$, $\lambda_{R^*E} \propto d_{R^*E}$. Therefore, the system SOP in the presence of a randomly distributed eavesdropper can be written as

$$\bar{P}_{out}(\gamma_S) = \mathbb{E}_{\mathrm{p}_E}\{P_{out}(\gamma_S, \mathrm{p}_E)\}, \quad (18)$$

where $P_{out}(\gamma_S, \mathrm{p}_E)$ is the expression of the SOP w.r.t. to the fixed location of E for different cases of combining schemes of SC or MRC at E. In the sequel, we first derive the expressions of the SOP w.r.t. a given location of E. Then (18) can be calculated by taking the expectation over the E's geometry environment of a circular disc of radius r_c.

A. Selection Combining

The asymptotic SOP for the SC scheme at E in case with friendly jamming is

$$\begin{aligned} P_{out}^{\mathrm{SC,J}}(\gamma_S, \mathrm{p}_E) &= 1 - \Pr\left\{\frac{\gamma_D}{\gamma_S} > \max\left(\gamma_{SE}, \gamma^{\mathrm{J}}_{R^*E}\right)\right\} \\ &= 1 - \mathbb{E}_{X,Y,\mathcal{J}}\left\{\Pr\left\{\begin{matrix} W < X\Upsilon_W(Y), \\ Z < \Upsilon_Z(Y,\mathcal{J}) \end{matrix}\right\}\right\}, \end{aligned} \quad (19)$$

where

$$\Upsilon_W(Y) = \frac{\varepsilon\lambda_{SR^*}\lambda_{R^*D}Y}{\gamma_S\lambda_{SE}(\varepsilon\lambda_{R^*D}Y+1)},$$
$$\Upsilon_Z(Y,\mathcal{J}) = \frac{\lambda_{R^*D}Y(1+P_J\lambda_{R^*E}\mathcal{J})}{\lambda_{R^*E}(\varepsilon\lambda_{R^*D}Y(\gamma_S-1)+\gamma_S)}.$$

Proposition 1. *With friendly jamming, the asymptotic SOP with respect to SC scheme at E is presented in* (20)*, at the top of the next page.*

Proof. Using the CDF and PDF of r.v. X and W, after some simplifications and employing [18, eq. (3.326,2)], we can derive (20) to complete the proof. □

B. Maximum-Ratio Combining

For the case of E using MRC scheme to increase intercepting level, the asymptotic SOP with friendly jamming is

$$\begin{aligned} P_{out}^{\mathrm{MRC,J}}(\gamma_S, \mathrm{p}_E) &= \Pr\left\{\frac{\gamma_D}{\gamma_S} < \gamma_{SE} + \gamma^{\mathrm{J}}_{R^*E}\right\} \\ &= \mathbb{E}_{X,Y,\mathcal{J}}\left\{\begin{matrix} \Pr\{Z > \Upsilon_Z(Y,\mathcal{J})\} \\ + \Pr\left\{\begin{matrix} Z < \Upsilon_Z(Y,\mathcal{J}), \\ W > X\Upsilon_W(Z,Y,\mathcal{J}) \end{matrix}\right\} \end{matrix}\right\}, \end{aligned} \quad (21)$$

where

$$\Upsilon_Z(Y,\mathcal{J}) = \frac{\lambda_{R^*D}Y(1+P_J\lambda_{R^*E}\mathcal{J})}{\lambda_{R^*E}(\varepsilon\lambda_{R^*D}Y(\gamma_S-1)+\gamma_S)},$$
$$\Upsilon_W(Y,Z,\mathcal{J}) = \frac{\varepsilon\lambda_{SR^*}}{\lambda_{SE}}\left(\frac{\lambda_{R^*D}Y}{\gamma_S(1+\varepsilon\lambda_{R^*D}Y)} - \frac{\lambda_{R^*E}Z}{\varepsilon\lambda_{R^*E}Z+1+P_J\lambda_{R^*E}\mathcal{J}}\right).$$

Proposition 2. *With friendly jamming, the asymptotic SOP with respect to MRC scheme at E is presented in* (22)*.*

Proof. Using the CDF and PDF of r.v. X and W, after some simplifications and employing [18, eq. (3.326,2)], we can derive (22) to complete the proof. □

Remark 1. To evaluate the SOP of the conventional AF relaying system (i.e., without jamming), the value of P_J can be set at zero and the expectation w.r.t $\mathcal{J}$ is eliminated in (19) and (21) to have the expressions of the system SOP.

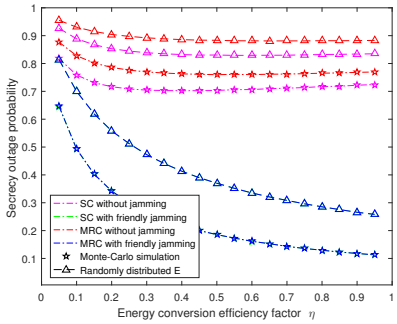
Remark 2. In the general case of a randomly distributed eavesdropper on ground inside a circular disc of radius r_c around S, although we cannot find the closed-form expression in this case, one can rely on numerical tools or apply the Jensen's inequality on (18) to effectively evaluate the lower bound SOP [19].

IV. Performance Evaluation

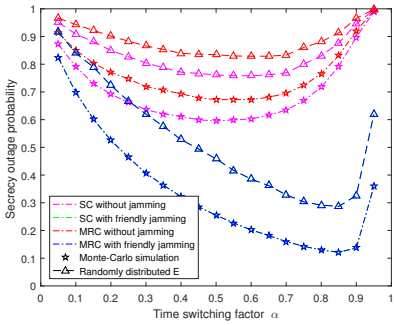
In this section, Monte-Carlo simulations of 10^5 runs are conducted to validate the theoretical expressions in (20) and (22) as well as to obtain insights into the secrecy performance of our system. We first set the target secrecy capacity at $C_{th} = 0.1$ bps/Hz. We assume that the jamming UAVs use all their harvested energy to effectively jam E, i.e., $\delta = 1$. For the purpose of illustration, all the coordinate systems in our simulations are shown in the cartesian coordinate, which are then converted to the polar coordinate to evaluate the analysis expressions. All the locations are shifted to the positive half of the coordinate system and presented in meters. S and D are fixed at $\mathrm{p}_S = (300, 300, 25)$ and $\mathrm{p}_D = (600, 300, 0)$, respectively. The aerial channel between UAVs and terrestrial base stations under shadowed-Rician fading of $(m_S, b, \Omega) = (5, 0.251, 0.279)$ for the average shadowing. The path loss

$$P_{out}^{\mathrm{SC,J}}\left(\gamma_S,\mathrm{p}_E\right)=1-U\sum_{l_X=0}^{m_S-1}\zeta_X\widetilde{\sum_u^{U-1}}\kappa_u\Gamma(l_X+\chi_u+1)\times\int_0^{\infty}f_{\mathcal{J}}\left(t\right)\int_0^{\infty}F_Z\left(\Upsilon_Z\left(y,t\right)\right)\left\{\left\{\eta_X+\eta_u\right\}^{-(l_X+\chi_u+1)}-\left\{\eta_X+\eta_u+\Upsilon_W\left(y\right)\right\}^{-(l_X+\chi_u+1)}\right\}f_Y\left(y\right)dydt \tag{20}$$

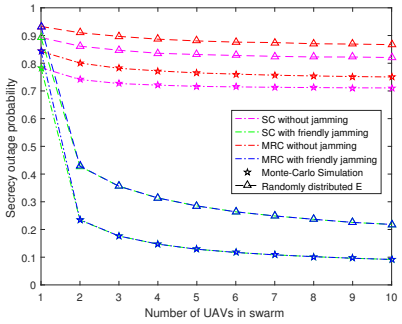
$$P_{out}^{\mathrm{MRC,J}}\left(\gamma_S,\mathrm{p}_E\right)=\int_0^{\infty}f_{\mathcal{J}}\left(t\right)\int_0^{\infty}\left\{1-F_Z\left(\Upsilon_Z\left(y,t\right)\right)\right\}f_Y\left(y\right)dydt+U\sum_{l_X=0}^{m_S-1}\zeta_X\widetilde{\sum_u^{U-1}}\kappa_u\Gamma(l_X+\chi_u+1)\times\int_0^{\infty}f_{\mathcal{J}}\left(t\right)\int_0^{\infty}f_Y\left(y\right)\int_0^{\Upsilon_Z(y,t)}\left\{\eta_X+\eta_u+\Upsilon_W\left(y,z,t\right)\right\}^{-(l_X+\chi_u+1)}f_Z\left(z\right)dzdydt \tag{22}$$



(a) SOP versus η.



(b) SOP versus α.



(c) SOP versus U.

Fig. 2: SOP versus (a) energy conversion efficiency factor; (b) TSR-AF factor; (c) number of UAVs in a swarm.

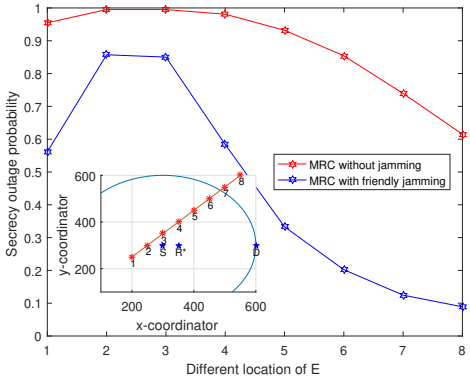


Fig. 3: SOP versus E's locations.

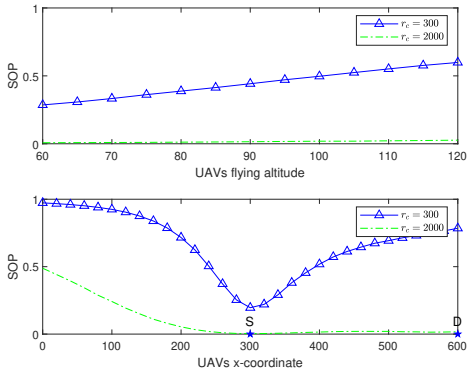


Fig. 4: SOP versus H_u, r_u of UAVs.

model is referred to a distance at $d_0 = 100$ meters where the reference $\rho_0 = 0$dB can be obtained using directional antennas or beamforming techniques, etc.

To illustrate the secrecy performance of the system, the SOP is investigated for two techniques of SC and MRC at E in a high SNR of $\psi = 40$dB. In these simulations, UAVs are hovering at $H_u = 60$ meters, in particular in a swarm at $\mathrm{p}_u = (350, 300, 60)$. Whereas E is assumed to be known and located at $\mathrm{p}_E = (600, 400, 0)$ or is randomly located around S inside a circular disk of $r_c = 300$ meters.

Fig. 2(a) and (b) show the impact of the energy conversion efficiency factor η and the TSR-AF factor α on the system SOP, when $U = 5$ UAVs in the swarm. Fig. 2(c) depicts the SOP vs. the number of UAVs when $\alpha = 0.8$ and $\eta = 0.8$. These figures validate the theoretical derivation in (20) and (22) as the coincidence between the asymptotic analysis and

the Monte Carlo simulation. Without friendly jamming, the SOP is not impacted much by increasing η or U in case of known E, i.e., the SOP is around 0.4 when $\eta \geq 0.25$ or $U \geq 3$. The relay selection not only provides the better link between S and D when the number of UAVs increases but also benefits the eavesdropping link from relaying UAV to E. Therefore, at a certain value of η and U, the signals received at E from UAVs are as good as at D, resulting in less variation in the SOP. With friendly jamming, the higher η or α, or the more UAVs in the swarm, more energy can be harvested to jam E. Therefore, the channels between UAVs and E are severely degraded, resulting in a significant decrease in the SOP. Increasing η and U provides the lower SOP, i.e., the SOP is around 0.1 when $\eta \geq 0.8$ or $U \geq 5$. From Fig. 2(b), increasing α at first gives more energy to AF the information and jam E, as such improves the SOP. However, the more the time for energy harvesting, the less the time for signal transmission. Therefore, α can be optimized to achieve the minimum SOP, e.g., $\alpha = 0.5$ without friendly jamming or $\alpha = 0.85$ with friendly jamming. Furthermore, the eavesdropper is the most effective in overhearing legitimate transmission using the MRC scheme. Without friendly jamming, the SOP in the case of the MRC scheme at E is greater than that of the SC scheme at E as expected. Using friendly jamming to degrade the channels between UAVs and E, results in the coincidence of two schemes. This implies signals from UAVs are not significant as compared to the signals from S.

Fig. 3 shows the significant impact of E's locations on the SOP. The particular locations of all nodes are illustrated on the subplot. E is assumed to change its location from $(550, 600, 0)$ to S, numbered from 1 to 8. The SOP increases as E gets closer to S (i.e., E's location numbered 2 and 3) and decreases when E goes far away from S. Locating around S helps E improve its capacity by boosting the link from S to E. Considering the general case of a randomly distributed E, the system SOP is calculated as the average SOP over the region around S in which E is randomly distributed. As expected, from Figs. 2(a), (b), (c), the SOP for this case is higher than the case when E is fixed far away from S. These figures also show that using UAVs to jam E, which is randomly distributed, provides the lower SOP as compared to the case without jamming.

The impact of UAVs' locations on the system SOP in the presence of a randomly distributed E is shown in Fig. 4. The flying altitude and x-coordinate of UAVs are independently investigated while other coordinates remain the same as above. Since higher flight altitudes lead to a more severe path loss for ground-to-air and air-to-ground communications, the SOP increases along with the higher flight altitude. Due to the path loss model, when the distance between S and R increases, UAVs receive lower SNR signals from S, and harvest less RF energy to relay signals to D as well as to jam E. Therefore, the SOP increases when UAVs fly at a high altitude and far from S. Moreover, as E is randomly distributed, we cannot exactly know the radius r_c of E's geometry environment. In Fig. 4, the SOP is high when E is distributed around S with $r_c = 300$, and significantly decreases when $r_c = 2000$.

V. Conclusions

In this paper, we proposed a cooperative friendly jamming in swarm UAV-assisted communications with wireless energy harvesting. The integral form of SOP was obtained for two popular detection schemes at the eavesdropper and verified by Monte-Carlo simulations. Using the SOP, we obtained engineering insights to optimize energy harvesting time, the number of UAVs in the swarm to achieve the required secrecy level.

References

[1] R. Ma, W. Yang, Y. Zhang, J. Liu, and H. Shi, "Secure mmWave communication using UAV-enabled relay and cooperative jammer," *IEEE Access*, vol. 7, pp. 119 729–119 741, 2019.

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

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

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

[5] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge: Cambridge University Press, 2005.

[6] B. Strassner and K. Chang, "Microwave power transmission: historical milestones and system components," *Proc. of the IEEE*, vol. 101, no. 6, pp. 1379–1396, 2013.

[7] M. Simic, C. Bil, and V. Vojisavljevic, "Investigation in wireless power transmission for UAV charging," *Procedia Comput. Sci.*, vol. 60, pp. 1846–1855, 2015.

[8] H. Yan, Y. Chen, and S.-H. Yang, "UAV-enabled wireless power transfer with base station charging and UAV power consumption," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 12 883–12 896, Nov. 2020.

[9] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.

[10] J. F. Paris, "Closed-form expressions for Rician shadowed cumulative distribution function," *Electron. Lett.*, vol. 46, no. 13, pp. 952–953, 2010.

[11] D. Zwillinger, V. Moll, I. Gradshteyn, and I. Ryzhik, "Special functions," in *Table of Integrals, Series, and Products*, 8th ed. Boston: Academic Press, 2014, pp. 1014–1059.

[12] V. Bankey and P. K. Upadhyay, "Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes," in *2017 IEEE VTC Spring*, 2017, pp. 1–5.

[13] D. Zwillinger, V. Moll, I. Gradshteyn, and I. Ryzhik, "Notation," in *Table of Integrals, Series, and Products*, 8th ed. Boston: Academic Press, 2014, pp. xli–xliii.

[14] M. Afshang and H. S. Dhillon, "Fundamentals of modeling finite wireless networks using binomial point process," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3355–3370, May 2017.

[15] D. N. K. Jayakody, T. D. P. Perera, A. Ghrayeb, and M. O. Hasna, "Self-energized UAV-assisted scheme for cooperative wireless relay networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 578–592, Jan. 2020.

[16] X. Yuan, Z. Feng, W. Ni, R. P. Liu, J. A. Zhang, and W. Xu, "Secrecy performance of terrestrial radio links under collaborative aerial eavesdropping," *IEEE Trans. Inf. Forens. Security*, vol. 15, pp. 604–619, 2020.

[17] H. Dang-Ngoc, D. N. Nguyen, K. Ho-Van, D. T. Hoang, E. Dutkiewicz, Q.-V. Pham, and W.-J. Hwang, "Secure swarm UAV-assisted communications with cooperative friendly jamming," 2021, arXiv:2107.14270.

[18] D. Zwillinger, V. Moll, I. Gradshteyn, and I. Ryzhik, "Definite integrals of elementary functions," in *Table of Integrals, Series, and Products*, 8th ed. Boston: Academic Press, 2015.

[19] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.

POINT-BY-POINT REPLY TO THE REVIEWERS' COMMENTS

Paper 40051

Paper title

Cooperative Friendly Jamming in Swarm UAV-assisted Communications with Wireless Energy Harvesting

Hanh Dang-Ngoc, Diep N. Nguyen, Dinh Thai Hoang, Khuong Ho-Van, Eryk Dutkiewicz

We would like to thank the TPC members, TPC chairs, and all the anonymous reviewers for the time and effort they devoted in reviewing our manuscript and providing us with various constructive comments and suggestions that helped us improve the quality of our work. In what follows, we provide our point-by-point response to each specific comment.

Reviewer 1

General comments: *The secrecy outage probability (SOP) of UAV-assisted amplify-and-forward relaying network with wireless energy harvesting with cooperative jamming has been derived by the authors. Selection combining and maximal ratio combining (MRC) techniques have been used at the eavesdropper. The paper is technically sound but the authors should take into perspective the following.*

Comments 1: *The closed-form expression of the asymptote of the SOP from equations (18) and (20) should be written in the paper.*

Reply: Thank you very much for your suggestion. We would like to clarify that the SOP expression in equations (18) and (20) is in its integral form. In the revised paper, we have made it clear by adding "we derive the expressions of the secrecy outage probability (SOP) in the integral form".

Comments 2: *The SOP expression is derived in a high SNR regime but it is not mentioned in the abstract or introduction or system model. The analysis performed should follow from the introduction and the authors should mention that they are deriving the expression in the high SNR regime.*

Reply: Thank you for your recommendation. We have added that the SOP expression is derived in a high SNR regime in both the abstract and introduction of the revised paper.

Comments 3: *Following from the point above, there is ambiguity as to whether the CSI of the eavesdropper is known or unknown. If known, the authors should follow the same assumption throughout the paper.*

Reply: Thank you for your recommendation. In the revised manuscript, we clarified that we consider both known and unknown CSI of the eavesdropper.

Comments 4: *The authors should take insights from Fig. 2 as to how SOP can be optimized for different parameters, e.g., No. of UAVs. etc (only α has been mentioned in the paper).*

Reply: Thank you for your recommendation. In the revised paper, we have provided discussion on the insights from Fig. 2 and how SOP can be used in different optimization problems.

Reviewer 2

General comments: In this paper, the authors have proposed cooperative friendly jamming in swarm UAV-assisted communications with wireless energy harvesting. The authors claim that the theoretical SOPs are derived and verified by Monte-Carlo simulations. Using the SOP, the authors have been shown to have obtained engineering insights to optimize energy harvesting time, the number of UAVs in the swarm to achieve the required secrecy level. The paper is well written but there are some questions that need to be addressed.

Comments 1: *In the abstract, the authors claim to have derived the analytical expression for SOP but in the manuscript, it is just a formulation and no closed-form or asymptotic analysis is presented.*

Reply: Thank you for your comment. By saying "closed form", we meant that the SOP's expression can be written in the integral form that is very convenient for numerical optimization problems. In the revised paper, to avoid the unnecessary confusion, we have clarified by adding that "we derive the expressions of the secrecy outage probability (SOP) in the integral form".

Comments 2: *Key contributions have not been highlighted by the authors.*

Reply: Thank you for your suggestion. In the revised manuscript, we have highlighted our key contributions in dot points.

Comments 3: *Key index should be in alphabetical order.*

Reply: Thank you for your suggestion. However, please allow us to order the key indices in terms of their importance and relevance to the paper's contributions.

Comments 4: *In the introduction and system model, the authors propose to have no knowledge about Eavesdropper's link but they have not considered the same during analysis.*

Reply: Thank you for your comment. In fact, we did consider the unknown CSI of the eavesdropper in the paper. To better highlight it, in the revised manuscript, we first presented the subsection of a general case of a randomly distributed eavesdropper, in which the SOP expressions have an expectation operation with respect to the location of the eavesdropper. Then the specific case of a fixed/known eavesdropper is presented in order to solve the general one.

Comments 5: *The authors must maintain consistency in assumptions throughout the paper.*

Reply: Thank you for your suggestion. We have thoroughly revised the paper to ensure its consistency.

Reviewer 3

Comments 1: *The concept of energy harvesting by relays and selecting a relay for transmission and other relays are jamming at the same time is a very old technique in physical layer security, in this respect the novelty of the work is limited. Authors also did not show any comparison with similar work in the introduction or in the results to show the novelty of the work. Literature survey should be improved.*

Reply: Thank you for your comment. We agree that there is a rich literature on relay selection and friendly jamming in physical layer security. However, our work is the first one to consider a swarm of UAV that can harvest energy and jam the eavesdropper. Moreover, one of the key contributions of our work is the derivation of the SOP that can facilitate various optimization of swarm UAV-aided communications scenarios.

In the revised paper, we have thoroughly revised the abstract, introduction, literature review to better highlight our contributions, compared with the literature. We also stated our contributions in dot points. We hope that the contributions of our work can be recognized.

Comments 2 and 3:

The derivations are not in the closed-form and the integral form with simulation does not show much design principle as claimed by the authors. There should have been simpler equations which should have been analyzed for appropriate optimization that authors mentioned.

The comment is not accurate: "To evaluate the secrecy rate, we derive the SOP and then ……."

Reply: Thank you for your comment. By saying "closed form", we meant that the SOP's expression can be written in the integral form that is very convenient for numerical optimization problems. In the revised paper, to avoid the unnecessary confusion, we have clarified by adding that "we derive the expressions of the secrecy outage probability (SOP) in the integral form".

Comments 4: *References must be in IEEE format.*

Reply: Thank you for your recommendation. In the revised paper, we have carefully checked the references to make sure that they are in the shortened IEEE format.

Reviewer 4

General comments: *The research paper utilizing cooperative, friendly jamming for swarm unmanned aerial vehicles is relevant to the conference.*

Comments 1: *As the derivation of SOP in MRC, as well as SC, is not complete (closed form), the authors may modify the sentences like: "We derive the expressions of the secrecy outage probability (SOP)" to "we present the expressions of the secrecy outage probability (SOP) in the integral form", "The theoretical SOPs were derived" to "Integral form of SOP was obtained." and other similar sentences to bring clarity from the reader's point of view.*

Reply: Thank you for your recommendation. In the revised paper, we have carefully revised the writing per your suggestions.

Comments 2: *The insights from SOP can be utilized to optimize energy harvesting time, the number of UAVs in the swarm to achieve the required secrecy level.*

Reply: Thank you very much for your suggestion. In the revised paper, we have carefully revised the writing per your suggestions.

Comments 3: *The authors can elaborate on the exact reason for the sentence after eqn. (16): "Since there are many factors in our model, the SOP cannot be directly analyzed for the case of a randomly distributed eavesdropper." and "Although we cannot find the closed-form expression in this case, one can rely on numerical tools or apply the Jensen's inequality on (22) to effectively evaluate the lower bound SOP [19]." after eqn. (22).*

Reply: Thank you for your comment. To clarify, in the revised manuscript, we first show a general case of a randomly distributed eavesdropper, in which the SOP expressions have an expectation operation with respect to the location of the eavesdropper. Then the SOP of the general case can be calculated by taking the expectation over the *E*'s geometry environment of a circular disc of radius r_c. This can be done using numerical tools.

Comments 4: *No insights from the equations can be made. The exact closed-form expressions of the lower limit, upper limit, or asymptotically high $(\eta, \alpha, U) $ may have provided better insights.*

Reply: Thank you for your recommendation. We agree with the reviewer that there should have been simpler equations which should have been analyzed. However, given the page limit, we can't add them all here. Instead, we plan add them to the journal version of the work where we have more space to discuss and provide more insights and results.