Secrecy-Energy Efficiency Performance of UAV-Enabled Communication Networks

Xiaohui Qi, Bin Li, Zheng Chu, Kaizhi Huang, and Hongbin Chen

Abstract

Recent researches show that unmanned aerial vehicle (UAV) can offer an efficient solution to achieve wireless connectivity with high mobility and low cost. This letter investigates the secrecy energy efficiency (SEE) in a multi-tier UAV-enabled communication network via a threshold-based access scheme and multi-antenna technique, where the UAV-enabled transmitters, legitimate receivers and eavesdroppers are deployed randomly. In particular, we first exploit the association probability of a randomly located receiver and the activation probability of UAV-enabled transmitters. Then, we analyze the security, reliability, and SEE of the UAV-enabled networks. Simulation results are provided to show the effect of the predetermined access threshold on the reliability as well as security performance, and determine the optimal design parameters for a given UAV-enabled network to maximize the SEE.

I. Introduction

In recent years, unmanned aerial vehicle (UAV) is emerging as a novel paradigm in civil and military applications, such as traffic monitoring, disaster rescue, and military reconnaissance [1]. In contrast to a terrestrial transmitter, UAV, as a mobile transmitter, can provide a promising solution to complement the capacity and coverage of terrestrial cellular systems, especially in extreme environments without infrastructure [2]. On the other hand, information security is a critical issue facing national defense when

X. Qi and K. Huang are with the National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China (e-mails: seven66226067@163.com; huangkaizhi@tsinghua.org.cn).

B. Li is with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China (e-mail: libin_sun@bit.edu.cn).

Z. Chu is with the School of Science and Technology, Middlesex University, London, NW4 4BT, U.K. (e-mail: z.chu@mdx.ac.uk).

H. Chen is with the Key Laboratory of Cognitive Radio and Information Processing, Guilin University of Electronic Technology, Ministry of Education, 1 Jinji Road, Guilin 541004, China (e-mail: chbscut@guet.edu.cn).

people rely heavily on wireless network for transmitting private information [3], [4]. Toward this, the use of UAV can offer new opportunities for security enhancement via a cooperative air-ground network. However, the performance and operation of a UAV-enabled communication network is constrained by the limited onboard energy. Therefore, the joint performance analysis of security and energy efficiency for UAV-enabled networks is urgently needed and is the emphasis of this work.

An overview of UAV-enable wireless communications was provided in [2], where the basic networking architecture and main channel characteristics were portrayed, and the key design challenges were discussed. Owing to high mobility, UAVs could also be deployed as mobile relays to provide wireless connectivity between distant ground terminals whose direct links were severely blocked [5]. The authors of [6] proposed an algorithm to allocate the time to different ground receivers based on the flying UAV's position to maximize the minimum throughput. [7] modeled the locations of the UAV base stations in a finite area as a uniform binomial point process and derived exact expression for the coverage probability of a target receiver situated on the ground. The aforementioned works addressed the basic networking architecture and optimization problem of the throughput. However, the information security against eavesdropping attacks was not taken into account.

A very recent effort [8] considered physical layer security in a UAV-enabled mobile relaying system where the air-to-ground link was established. Note that the authors of [8] focused on the optimization of transmit power, but not from the perspective of network analysis and deployment. They considered neither the multi-UAV multi-eavesdropper wiretap scenarios, nor the random spatial positions of network nodes. To the best of our knowledge, such work has not tried to design and analyze the secrecy energy efficiency (SEE) performance in UAV-enable communication networks, which motivates this work.

In this letter, we focus on the SEE in downlink UAV-enabled communication networks. Main contributions of this letter are summarized as follows. 1) Modeling multi-antenna UAV-enabled transmitters, receivers, and eavesdroppers as independent homogeneous Poisson point processes (HPPPs). By using the threshold-based access scheme, a fundamental analysis framework for evaluating the SEE performance in UAV-enabled communication networks is proposed; 2) The influences on connection outage probability (COP) and secrecy outage probability (SOP), caused by the predetermined access threshold and the number of receivers served by each transmitter, are further analyzed in this scenario.

Notations: Boldface lowercase letter denotes vector. $(\cdot)^{\dagger}$, $\|\cdot\|$, $\mathbb{P}\{\cdot\}$, and $\mathbb{E}(\cdot)$ denote the conjugate transpose, Euclidean norm, probability, and expectation operation. $\Gamma(a,b)$ is the Gamma distribution with shape parameter a and scale parameter b.

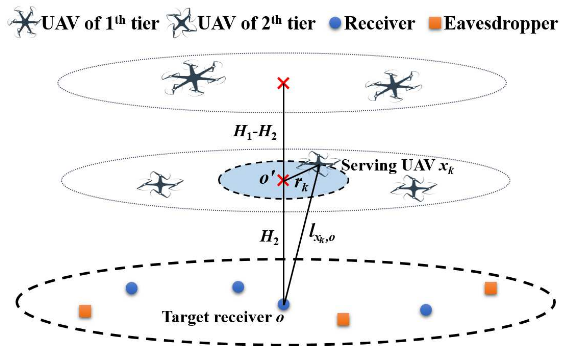


Fig. 1: A simplified system model for a 2-tier UAV-enabled communication network.

II. Downlink System Model

A. Network Descriptions

We consider a wireless system consisting of K-tier UAV-enabled transmitters, multiple legitimate receivers, and multiple eavesdroppers, as shown in Fig. 1. Note that the UAVs of the k^{th} tier are assumed to be at the same height H_k for simplicity of exposition. Let $\kappa \triangleq \{1, 2, \ldots, K\}$ denote the set of UAVs. In the k^{th} tier, each UAV-enabled transmitter equipped with M_k antennas can collect and transmit information to the ground receivers. The number of receivers served in each transmitter's resource block is Ψ_k, and the transmit power is P_k. The legitimate receivers and eavesdroppers are equipped with a single antenna. We denote the set of UAVs in the k^{th} tier, legitimate receivers, and eavesdroppers locations as Φ_k, Φ_u, and Φ_{E}, which follow independent HPPPs with densities λ_k, λ_u, and λ_{E}, respectively. According to Slivnyak's theorem [9], the analysis can be performed at a typical legitimate receiver located at the origin. Compared with interference, noise almost has no effect for legitimate receivers in multi-tier wireless networks [10]. Hence, we assume that the noises received by legitimate receivers and eavesdroppers are neglected.

In this letter, the system model has other three restraints:

- All the channels undergo independent and identically distributed quasi-static Rayleigh fading;
- Perfect channel state information (CSI) is available at each UAV-enabled transmitter;
- All the transmitters use precoding $\mathbf{w} = \mathbf{h}^{\dagger}/\|\mathbf{h}\|$, where $\mathbf{h}$ is the corresponding channel.

In UAV-enabled communication networks, the received signal-interference-plus-noise ratio (SINR) of the typical receiver o served by the UAV-enabled transmitter $x_k \in \Phi_k$ in the k^{th} tier is given by

$$\mathrm{SINR}_u^k = \frac{P_k h_{x_k,o} \|l_{x_k,o}\|^{-\alpha}}{I_{o,k}^{\mathrm{inter}}} \tag{1}$$

where $P_k h_{x_k,o} \|l_{x_k,o}\|^{-\alpha}$ denotes the received power of the k^{th} receiver, $l_{x_k,o} = \sqrt{H_k^2 + r_{x_k,o}^2}$ denotes the distance between the serving transmitter x_k and o, $r_{x_k,o}$ denotes the distance between x_k and o' (the center of the plane of Φ_k), $h_{x_k,o} \sim \Gamma(\Delta_k, 1)$ stands for the array gain of the main channel, $\Delta_k = M_k - \Psi_k + 1$, and $\|l_{x_k,o}\|^{-\alpha}$ is the path loss [11]. $I_{o,k}^{\text{inter}} = \sum_{i \in \mathcal{K}} \sum_{y_i \in \Phi_i^o \setminus x_k} P_i g_{o,i} \|l_{y_i,o}\|^{-\alpha}$ represents receiver's received interference from all the active transmitters, where $l_{y_i,o} = \sqrt{H_i^2 + r_{y_i,o}^2}$ denotes the distance between the transmitter y_i and o, $r_{y_i,o}$ denotes the distance between y_i and o', and $g_{o,i} \sim \Gamma(\Psi_i, 1)$ is the array gain of corresponding interference channel. The set of active transmitters in the i^{th} tier is a thinning of Φ_i, denoted by Φ_i^o with density $\lambda_i^o = P_{\text{act}}^i \lambda_i$, where P_{act}^i denotes the activation probability of transmitters in the i^{th} tier.

We consider the non-colluding and passive eavesdropping scenario that each eavesdropper intercepts the information signal of typical receiver independently without any attacks. In this case, we only pay our attention to the eavesdropper that has the largest received SINR, which was commonly assumed [11]. Such an eavesdropper e is considered as the most malicious one and its received SINR can be expressed as

$$\text{SINR}_e^k = \max_{x_e \in \Phi_{\text{E}}} \left\{ \frac{P_k h_{x_e,k} \|l_{x_e,k}\|^{-\alpha}}{I_{x_e,k}^{\text{intra}} + I_{x_e,k}^{\text{inter}}} \right\} \tag{2}$$

where $h_{x_e,k} \sim \exp(1)$ denotes the equivalent small-scale fading channel power gain for the received SINR of eavesdropper $x_e \in \Phi_{\text{E}}$, $l_{x_e,k} = \sqrt{H_k^2 + r_{x_e,k}^2}$ indicates the distance between the eavesdropper x_e and its target transmitter x_k, and $r_{x_e,k}$ is the eavesdropper's horizontal distance from x_k. $I_{x_e,k}^{\text{intra}} = P_k g_{x_e,k} \|l_{x_e,k}\|^{-\alpha}$ with $g_{x_e,k} \sim \Gamma(\Psi_k - 1, 1)$ and $I_{x_e,k}^{\text{inter}} = \sum_{i \in \mathcal{K}} \sum_{y_i \in \Phi_i^o \setminus x_k} P_i g_{x_e,y_i} \|l_{x_e,y_i}\|^{-\alpha}$ with $g_{x_e,y_i} \sim \Gamma(\Psi_i, 1)$ are intra-cell and inter-cell interference, respectively [11]. $l_{x_e,y_i} = \sqrt{H_i^2 + r_{x_e,y_i}^2}$ is the distance between the eavesdropper x_e and transmitter y_i, and r_{x_e,y_i} is the eavesdropper's horizontal distance from y_i.

B. Secrecy mobile association scheme

In this subsection, we assume open access, i.e., a legitimate receiver is permitted to access any tier's UAV-enabled transmitters. In addition, we consider a mobile association based on highest average received signal power (ARSP), where a legitimate receiver is only allowed to associate with the UAV-enabled transmitter providing the highest ARSP. For a legitimate receivers o, the ARSP related to the k^{th} tier is defined as $\bar{P}_k = P_k \Delta_k l_{x_k,o}^{-\alpha}$.

Following the idea of [12], the secure mobile association scheme is designed for improving the security/reliability of downlink transmission in UAV-enabled communication networks. For the secure mobile association scheme, the served transmitter broadcasts data only when the truncated ARSP at receiver is larger than a predetermined access threshold τ, i.e. $l_{x_k,o} \leq R_k = (P_k \Delta_k/\tau)^{\frac{1}{\alpha}}$, where R_k denotes the radius of the serving region. The following lemma provides the association probability.

Lemma 1: The probability with which a typical legitimate receiver o associates with a transmitter in the k^{th} tier is given as

$$\begin{aligned} S_k = & \int_0^{\sqrt{R_k^2-H_k^2}} \prod_{j\in\kappa\backslash k} \mathbb{P}\left\{ \frac{P_k\Delta_k\left(H_j^2+r_{x_j}^2\right)^{\alpha/2}}{P_j\Delta_j(H_k^2+x^2)^{\alpha/2}} > 1 \,|r_{x_k} \right\} f_{r_{x_k}}(x)\,\mathrm{d}x \\ \overset{(a)}{=} & \frac{\exp\left[-\pi \sum\limits_{j\in\kappa\backslash k} \lambda_j \left(\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha} H_k^2 - H_j^2\right)\right]}{\sum\limits_{j\in\kappa} \hat{\lambda}_{j,k}\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}} - \frac{\exp\left[-\pi \sum\limits_{j\in\kappa} \lambda_j \left(\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha} R_k^2 - H_j^2\right)\right]}{\sum\limits_{j\in\kappa} \hat{\lambda}_{j,k}\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}}, \end{aligned} \tag{3}$$

where the step (a) can be easily recognized by the probability generating functional of HPPP [12], $f_{r_{x_k}}(x) = 2\pi\lambda_k x e^{-\pi\lambda_k x^2}$, r_{x_i} is the receiver's horizontal distance from transmitter x_i, $\hat{P}_{i,j} = P_i/P_j$, $\hat{\Delta}_{i,j} = \Delta_i/\Delta_j$, and $\hat{\lambda}_{i,j} = \lambda_i/\lambda_j$.

It is worth noting that a transmitter in the k^{th} tier may be active when existing an associated receiver, and the activation probability of transmitter B_k is defined as [12]

$$\begin{aligned} P_{\text{act}}^k &= \mathbb{P}\left(B_k \text{ associates with at least one receiver}\right) \\ &= 1 - \mathbb{E}_{\Phi_u}\left[\prod_{x_u\in\Phi_u} \mathbb{P}\left(x_u \text{ is not associated with } B_k\right)\right]. \end{aligned} \tag{4}$$

From (1) and (2), we know that the derivation for activation probability of transmitter is necessary, which is given in Lemma 2.

Lemma 2: The activation probability of UAV-enabled transmitters in the k^{th} tier is given by

$$\begin{aligned} P_{\text{act}}^k &= 1 - \mathbb{E}_{\Phi_u}\left[\prod_{x_u\in\Phi_u} \mathbb{P}\left\{ \frac{P_k\Delta_k}{l_{x_u,B_k}^{\alpha}} < \max_{j\in\kappa} P_j\Delta_j l_{x_j,x_u}^{-\alpha} \right\}\right] \\ &\overset{(b)}{=} 1 - \exp\left[-2\pi\lambda_u \int_{H_k}^{R_k} e^{-\pi \sum\limits_{j\in\kappa} \lambda_j \left(\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha} x^2 - H_j^2\right)} x\mathrm{d}x\right] \\ &= 1 - \exp\left[\frac{e^{-\pi \sum\limits_{j\in K} \lambda_j \left(R_k^2\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha} - H_j^2\right)}}{\lambda_\mu^{-1} \sum\limits_{j\in\kappa} \lambda_j\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}} - \frac{e^{-\pi \sum\limits_{j\in K} \lambda_j \left(H_k^2\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha} - H_j^2\right)}}{\lambda_\mu^{-1} \sum\limits_{j\in\kappa} \lambda_j\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}}\right], \end{aligned} \tag{5}$$

where the step (b) is derived following the basic nature of PPP, l_{x_u,B_k} is the distance between x_u and B_k, and l_{x_j,x_u} is the distance between x_u and x_j.[1]

[1]For convenience, we interchangeably use $\exp(x)$ and e^x to denote the exponential function of x.

III. Performance analysis

In this section, we analyze the SEE in UAV-enabled communication networks. In an effort to assess the SEE, we first derive the COP and the SOP in UAV-enabled networks.

When the legitimate receiver's message cannot be decoded with error-free, the connection outage occurs. The expression of COP in the k^{th} tier is given in Theorem 1.

Theorem 1: When the typical receiver is associated with a UAV-enabled transmitter in the k^{th} tier, its COP can be expressed as

$$P_{\text{cop}}^{k}\left(\gamma_k\right) = \mathbb{P}\left(\text{SINR}_u^k < 2^{\gamma_k} - 1\right) = F_{\text{SINR}_u^k}\left(2^{\gamma_k} - 1\right), \tag{6}$$

where γ_k is the target channel capacity. The cumulative distribution function (CDF) of SINR_u^k can be given by

$$\begin{aligned} F_{\text{SINR}_u^k}(\gamma) = 1 - \tfrac{\pi\lambda_k}{S_k}\textstyle\sum_{n=0}^{\Delta_k-1}\frac{1}{n!}\left(\frac{\gamma}{P_k}\right)^n \sum_{\bar{m}\in M(n)} C(\bar{m})F(\bar{m})\Gamma\left(\sum m_l + 1\right) \\ \times \textstyle\sum_{i=0}^{\sum m_l} \frac{\left(e^{-Q_k(\gamma)R_k^2}R_k^{2\left(\sum m_l - i\right)} - e^{-Q_k(\gamma)H_k^2}H_k^{2\left(\sum m_l - i\right)}\right)}{\left[-Q_k(\gamma)\right]^{i+1}\Gamma\left(\sum m_l + 1 - i\right)e^{-\pi\sum\limits_{j\in\kappa}\lambda_j\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}H_k^2}}, \end{aligned} \tag{7}$$

where $M\left(n\right) = \{\bar{m} = \left(m_1, m_2, \cdots, m_n\right)^{\text{T}} : \sum\limits_{j=1}^{n} j m_j = n\}$, $u_{j,k} = \left(1 + \gamma/(\hat{\Delta}_{j,k}\hat{B}_{j,k})\right)^{-1}$, $C\left(\bar{m}\right) = \frac{n!}{\prod_j\left(m_j!(j!)^{m_j}\right)}$, $Q_k\left(\gamma\right) = \sum\limits_{j\in\kappa}\lambda_j^o\tilde{C}_{j,k}(\gamma\hat{P}_{j,k})^{2/\alpha} + \pi\sum\limits_{j\in\kappa}\lambda_j\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}$, $F\left(\bar{m}\right) = \frac{\prod\limits_{l=1}^{n}\left(\sum\limits_{j\in\kappa}D_j(l)P_j^{\frac{2}{\alpha}}\right)^{m_l}}{\left(\gamma P_k^{-1}\right)^{-\frac{2}{\alpha}\sum m_l + n}(2\pi)^{-\sum m_l}}$, $\tilde{C}_{j,k} = \frac{2\pi}{\alpha}\sum\limits_{m=1}^{\Psi_j}\begin{pmatrix}\Psi_j\\ m\end{pmatrix}B'\left(\Psi_j - m + \frac{2}{\alpha}, m - \frac{2}{\alpha}, u_{j,k}\right)$, $\hat{B}_{i,j} = B_i/B_j$, $B_i = \sqrt{\Psi_i/\Delta_i}$, $B'\left(a, b, z\right) = \int_z^1 t^{a-1}(1-t)^{b-1}dt$ is the Beta function, and $D_j(l) = \frac{\lambda_j^o}{\alpha}\frac{B'\left(\Psi_j + \frac{2}{\alpha}, l - \frac{2}{\alpha}, u_{j,k}\right)}{((\Psi_j + l - 1)!)^{-1}(\Psi_j - 1)!}$.

Proof: The CDF of SINR_u^k can be obtained as

$$\begin{aligned} F_{\text{SINR}_u^k}\left(\gamma\right) &= 1 - \int\limits_0^{\sqrt{R_k^2 - H_k^2}} \mathbb{P}\left(h_{x_k,o} > \frac{\gamma I_{o,k}^{\text{inter}}}{P_k\left\|l_{x_k,o}\right\|^{-\alpha}}\,|r_{x_k,o}\right) f_{r_{x_k,o}}\left(x\right)\mathrm{d}x \\ &= 1 - \int\limits_{H_k}^{R_k}\sum_{n=0}^{\Delta_k - 1}\frac{\mathrm{d}^n L_{I_{o,k}^{\text{inter}}}(s)}{\mathrm{d}s^n}\frac{2y\pi\lambda_k(n!)^{-1}(-s)^n S_k^{-1}}{e^{\pi\sum\limits_{j\in\kappa}\lambda_j\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}\left(y^2 - H_k^2\right)}}\mathrm{d}y, \end{aligned} \tag{8}$$

where $L_{I_{o,k}^{\text{inter}}}\left(s\right) = \prod\limits_{i\in\kappa}\exp\left[\int_{\left(\hat{P}_{i,k}\hat{\Delta}_{i,k}\right)^{\frac{1}{\alpha}}y}^{\infty} 2\pi\lambda_i^o\left(1 - \left(1 + sP_i z^{-\alpha}\right)^{-1}\right)z\mathrm{d}z\right]$ is obtained by the basic nature of PPP, $f_{r_{x_k,o}}\left(x\right) = \frac{2\pi\lambda_k x}{S_k}e^{-\pi\sum\limits_{j\in\kappa}\lambda_j\left(\hat{P}_{j,k}\hat{\Delta}_{j,k}\right)^{2/\alpha}x^2}$, $s = \gamma P_k^{-1}y^{\alpha}$, and $\frac{\mathrm{d}^n L_{I_{o,k}^{\text{inter}}}(s)}{\mathrm{d}s^n}$ is derived in [12]. Substituting (8) into (6), we complete the proof.

Mathematically, the COP of a typical receiver can be given by $P_{\text{cop}} = \sum\limits_{k\in\kappa} S_k P_{\text{cop}}^{k}\left(\gamma_k\right)$.

As such, when the eavesdroppers have a better channel than the access threshold, the secrecy outage occurs to ensure the secrecy of those messages. As an important indicator of security, the expression of SOP in the k^{th} tier is given in Theorem 2.

Theorem 2. When the typical receiver is associated with a UAV-enabled transmitter in the k^{th} tier, its SOP can be given by

$$P_{\mathrm{sop}}^{k}\left(\hat{R}_s^k\right) = \mathbb{P}\left(\log_2\left(1+\mathrm{SINR}_e^k\right) > \gamma_k - \hat{R}_s^k\right) = 1 - F_{\mathrm{SINR}_e^k}\left(2^{\gamma_k - \hat{R}_s^k} - 1\right), \tag{9}$$

where $\hat{R}_s^k$ is the target secrecy rate of $P_{\mathrm{sop}}^{k}\left(\hat{R}_s^k\right)$ and the CDF of SINR_e^k can be expressed as

$$F_{\mathrm{SINR}_e^k}(\gamma) = \exp\left[-2\pi\lambda_{\mathrm{E}}(\gamma+1)^{-(\Psi_k-1)} \times \int\limits_{H_k}^{\infty} e^{-\sum\limits_{i\in\kappa}\int_{H_i}^{\infty} 2\pi\lambda_i^o\left(1-\left(1+\frac{\gamma P_i y^{\alpha}}{P_k z^{\alpha}}\right)^{-\Psi_i}\right) z dz} y \mathrm{d}y\right] \tag{10}$$

Proof: The CDF of SINR_e^k can be derived as follows:

$$\begin{aligned} F_{\mathrm{SINR}_e^k}(\gamma) &= \mathbb{E}_{\Phi_{\mathrm{E}}}\left[\prod_{x_e\in\Phi_{\mathrm{E}}} \mathbb{P}\left(h_{x_e,k} \le \frac{\gamma\left(I_{x_e,k}^{\mathrm{intra}} + I_{x_e,k}^{\mathrm{inter}}\right)}{P_k\|l_{x_e,k}\|^{-\alpha}}\right)\right] \\ &\overset{\text{(c)}}{=} \exp\left(-2\pi\lambda_{\mathrm{E}}\int_{H_k}^{\infty} L_{I_{x_e,k}^{\mathrm{intra}}}(s)\, L_{I_{x_e,k}^{\mathrm{inter}}}(s)\, y\mathrm{d}y\right), \end{aligned} \tag{11}$$

where the step (c) is achieved by the probability generating functional of HPPP Φ_{E} [12], the Laplace transform of $I_{x_e,k}^{\mathrm{inter}}$ and $I_{x_e,k}^{\mathrm{intra}}$ are given by $L_{I_{x_e,k}^{\mathrm{inter}}}(s) = e^{-\sum\limits_{i\in\kappa} 2\pi\lambda_i^o \int_{H_i}^{\infty}\left(1-\left(1+sP_i z^{-\alpha}\right)^{-\Psi_i}\right) z \mathrm{d}z}$ and $L_{I_{x_e,k}^{\mathrm{intra}}}(s) = (\gamma+1)^{-(\Psi_k-1)}$, respectively. Substituting (11) into (9), we can arrive at the final result.

Mathematically, the SOP of a typical receiver can be given by $P_{\mathrm{sop}} = \sum\limits_{k\in\kappa} S_k P_{\mathrm{sop}}^{k}\left(\hat{R}_s^k\right)$.

Due to the requirement of secure communication and the limitation of energy, SEE as an important metric is used to evaluate the secrecy performance achieved with unit energy consumption. Similar to [13], SEE is defined as the ratio of the average secrecy rate at which the confidential messages are reliably and securely transmitted from the UAV-enabled transmitters to the intended receivers over the total power consumption (bits/Joule). The following theorem provides the SEE achieved by the UAV-enabled communication network.

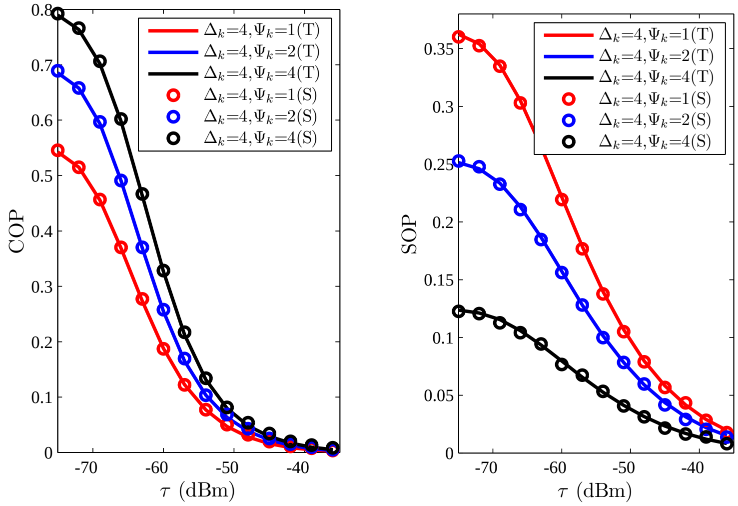
Theorem 3. The SEE of the UAV-enabled communication networks is given by

$$\mathrm{SEE} = \sum_{k\in\kappa} S_k \mathrm{SEE}_k, \tag{12}$$

where

$$\mathrm{SEE}_k = \frac{\Psi_k\left(1-P_{\mathrm{cop}}^{k}(\gamma_k)\right)\left(1-P_{\mathrm{sop}}^{k}\left(\hat{R}_{s,k}\right)\right)\hat{R}_{s,k}}{P_k^{\mathrm{total}}} \tag{13}$$

denotes the SEE for the k^{th} tier. The total power consumption for a UAV-enabled transmitter in each channel is given by $P_k^{\mathrm{total}} = P_k^0 + \frac{P_k}{\varepsilon_k} + \sum\limits_{t=1}^{3}\left(\Psi_k^{t-1}\left(\tilde{\Delta}_t^k + M_k\Lambda_t\right)\right)$ [13]. P_k^0 and ε_k represent the static



(a) COP versus τ (b) SOP versus τ

Fig. 2: The COP and SOP versus τ with $P_1 = 15\text{dBm}$ and $P_2 = 5\text{dBm}$. S denotes the simulation results and T denotes the theoretical results.

hardware power consumption and the efficiency of the power amplifier for the k^{th} tier, respectively. The parameters $\tilde{\Delta}_t^k$ and Λ_t depends on the transceiver chains, coding and decoding, etc.

IV. Numerical Results

In this section, numerical results are provided to examine the COP and SOP for a 2-tier UAV-enabled networks. In addition, the impact of τ and P_1 on the SEE are also investigated. The validity of the theoretical derivations are verified by the Monte Carlo simulation results. In the following results, we assume $\alpha = 4$, $\lambda_1 = 1.5 \times 10^{-5}\text{m}^2$, $\lambda_2 = 3 \times 10^{-5}\text{m}^2$, $\lambda_u = 6 \times 10^{-6}\text{m}^2$, $\lambda_{\text{E}} = 2 \times 10^{-5}\text{m}^2$, $H_1 = 13\text{m}$, $H_2 = 5\text{m}$, $\varepsilon_1 = \varepsilon_2 = 0.38$, $\tilde{\Delta}_1^k = 4.8$, $\tilde{\Delta}_2^k = 0$, $\tilde{\Delta}_3^k = 2.08\Psi_k \times 10^{-8}$, $\Lambda_1 = 1$, $\Lambda_2 = 9.5 \times 10^{-8}$, $\Lambda_3 = 6.25 \times 10^{-8}$, $P_1^0 = 4\text{W}$, and $P_2^0 = 13.6\text{W}$. All the simulation results shown in this section are averaged over 100,000 Monte Carlo simulations.

Fig. 2 compares the SOP and COP in UAV-enabled networks with different Ψ_k ($k \in \{1, 2\}$). Intuitively, the simulation results highly consistent with the theoretical results, which validates the accuracy of those two analytical expressions derived. It is also observed that the COP increases with Ψ_k and the SOP decreases with Ψ_k, which is mainly due to the fact that Ψ_k not only increases the interference received by eavesdroppers, but also increases the interference received by legitimate receivers. Furthermore, the

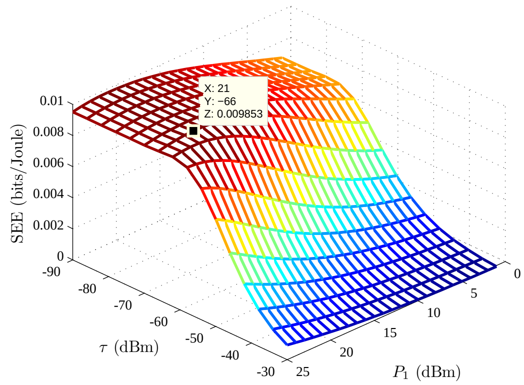


Fig. 3: SEE versus τ and P_1, with $\Psi_1 = \Psi_2 = 1$, $\Delta_1 = 4$, $\Delta_2 = 2$ and $P_2 = 5$dBm.

COP and SOP performances over different τ are also shown in Fig. 2. Obviously, both SOP and COP degrades with increasing τ. This implies that the predetermined access threshold can affect both security and reliability. This is due to both the association probability and the activation probability of UAV-enabled transmitter degrades with increasing τ.

Fig. 3 shows the influences on SEE caused by τ and P_1. From (12), we note that the SEE is not a monotonous function of τ and P_1. Consequently, the optimal value of SEE can be obtained by properly designing τ and P_1. In Fig. 3, the SEE reveals a maximum value for a given network with the optimal pair of $(\tau, P_1) = (-66, 21)$, which is marked in the figure.

V. Conclusion

In this letter, we studied the SEE of downlink UAV-enabled networks, where the locations of network nodes were characterized by independent HPPPs. To ensure the reliability and security of UAV-enabled networks, both the threshold-based access scheme and multi-antenna technology were employed. The security, reliability, and SEE of UAV-enabled networks was analyzed. Simulation results have revealed that the reliability and security of UAV-enabled networks can be improved by using the threshold-based access scheme, and the optimal value of SEE can be achieved by designing the transmit powers and predetermined access threshold.

References

[1] Y. Zhou, N. Cheng, N. Lu, and X. S. Shen, “Multi-UAV-aided networks: Aerial-ground cooperative vehicular networking architecture,” *IEEE Veh. Technol. Mag.*, vol. 10, no. 4, pp. 36-44, Dec. 2015.

[2] 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.

[3] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283-297, Jan. 2016.

[4] B. Li, Z. Fei, and H. Chen, "Robust articial noise-aided secure beamforming in wireless-powered non-regenerative relay networks," *IEEE Access*, vol. 4, pp. 7921-7929, Nov. 2016.

[5] J. Lyu, Y. Zeng, R. Zhang, and T. J. Lim, "Placement optimization of uav-mounted mobile base stations," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 604-607, Mar. 2017.

[6] J. Lyu, Y. Zeng, and R. Zhang, "Cyclical multiple access in uav-aided communications: A throughput-delay tradeoff," *IEEE Wireless Commun. Lett.*, vol. 5, no. 6, pp. 600-603, Dec. 2016.

[7] V. V. C. Ravi and H. S. Dhillon, "Downlink coverage probability in a nite network of unmanned aerial vehicle (UAV) base stations," in *Proc. IEEE SPAWC*, Edinburgh, UK, Jul. 2016, pp. 1-5.

[8] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, published online.

[9] D. B. Taylor, H. S. Dhillon, T. D. Novlan, and J. G. Andrews, "Pairwise interaction processes for modeling cellular network topology," in *Proc. IEEE GLOBECOM*, Anaheim, USA, Dec. 2012, pp. 4524-4529.

[10] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 550-560, Apr. 2012.

[11] Y. Deng, L. Wang, K.-K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, "Safeguarding massive MIMO aided hetnets using physical layer security," in *Proc. IEEE WCSP*, Nanjing, China, Oct. 2015, pp. 1-5.

[12] H.-M. Wang, T.-X. Zheng, J. Y. D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204-1219, Mar. 2016.

[13] J. Ouyang, M. Lin, Y. Zou, W.-P. Zhu, and D. Massicotte, "Secrecy energy efciency maximization in cognitive radio networks," *IEEE Access*, vol. 5, pp. 2641-2650, Mar. 2017.