International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 6, December 2023, pp. 6410~6418
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i6.pp6410-6418

Secrecy performance analysis on spatial modeling of wireless communications with unmanned aerial vehicle and ground devices

Cuu Ho Van[1], Hong-Nhu Nguyen[1], Si-Phu Le[2], Miroslav Voznak[2]
[1]Faculty of Electronics and Telecommunications, Saigon University, Ho Chi Minh City, Vietnam
[2]Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, Ostrava, Czech Republic

Article Info

Article history:

Received Feb 17, 2023
Revised May 18, 2023
Accepted May 23, 2023

Keywords:

Intercept probability
Physical layer security
Secrecy outage probability
Stochastic geometry
Unmanned aerial vehicle

ABSTRACT

In this paper, the secrecy performance of the spatial modeling for ground devices with randomly placed eavesdroppers when an unmanned aerial vehicle (UAV) acted as two hops decode and forward (DF) was investigated. We characterize the secrecy outage probability (SOP) and intercept probability (IP) expressions. Our capacity performance analysis is based on the Rayleigh fading distributions. After analytical results by Monte Carlo simulation, and the Gauss-Chebyshev parameter was selected to yield a close approximation, the results demonstrate the SOP with the average signal-to-noise ratio (SNR) between UAV and ground users among the eavesdroppers and the IP relationship with the ability to intercept the information of the ground users successfully.

Corresponding Author:

Hong-Nhu Nguyen
Faculty of Electronics and Telecommunications, Saigon University
273 An Duong Vuong Street, Ward 3, District 5, 70 000, Ho Chi Minh City, Vietnam
Email: nhu.nh@sgu.edu.vn

1. INTRODUCTION

Unmanned aerial vehicles (UAVs) have used popularity in the world, in which superiorities of quad-copter UAVs, which were well introduced in recently published studies, included: adaptive altitude flight control, vertically moving and landing on moving targets via disturbance observer-based controllers. Furthermore, UAVs have become a vital link between the internet of things (IoT) and cellular systems in 5G communication technologies [1], [2]. The preference for UAVs in emerging IoT communications can be attributed to the dominant line-of-sight (LoS) links and mobility; therefore, making UAV-aided communication very desirable [3], [4]. However, the prevalence of these strong LoS links makes UAV-aided communications vulnerable to ground/aerial eavesdroppers, consequently ensuring privacy and data security becomes very crucial [5].

Several research works such as [6], [7], have proposed different solutions for securing various kinds of UAV-assisted networks. In [5], the secrecy outage analysis of UAV-aided two-hop decode and forward (DF) relay cognitive transmission with energy harvesting under Nakagami-m channel conditions was investigated. On the basis of closed-form expressions of non-zero secrecy capacity probability and optimal secrecy outage probability (SOP), the study examined where there is no channel state information (CSI) for eavesdropper. Furthermore, in the simulation results, it was proved that the system secrecy capacity commits to be increased by optimizing the power dividing factor and other parameters simultaneously. Differently in Ji *et al.* [6] analyzing the functions was employed to derive the closed-form expressions of the system SOP and the probability of non-zero secrecy capacity for a cognitive network DF UAV-assisted relay transmission with energy harvesting. Li *et al.* [7] studied the secrecy energy efficiency maximization problem in full-duplex (FD) UAV-assisted wireless sensor networks (WSNs) with eavesdroppers without CSI. The result depends on the restrictions of connection outage probability (COP), SOP, safely collected bits, and flight trajectory. To deal with the non-convex difficulty, two important steps were taken. In the first step, the optimal code word ratio and the redundancy ratio in closing expressions were inferred. In the next step, an algorithm with low complication was established utilizing block coordinate reduction (BCD) method to develop the replacement of sensor nodes (SNs) scheduling, SN transmitter power, UAV transmit power and UAV trajectory.

Moreover, the research [8]–[11] investigated the impact of multiple eavesdroppers on SOP. Liu *et al.* [8] examined the SOP obtained by forwarding it to a low-altitude UAV large stable transmission system with the existence of numerous UAV eavesdroppers utilizing maximum ratio combining for intercepting legitimate UAV-transmitter and UAV-relay transmissions. The authors derived closed-form expressions for the SOP in regarding the UAV participation, backhaul dependability, eavesdropping probability, and Nakagami-m fading parameters. The possibility of asymptotic secret loss is also inferred in the area with a high signal-to-noise rate. It is found that the secrecy variety obtained by forwarding is collectively concluded by the UAV cooperation and structure elements of Nakagami-m fading links in the main channel. Bao *et al.* [9], the SOP of a UAV-aided relay communication system, where the UAV relay transmits information from a ground base station (GBS) to legitimate ground users in the presence of multiple aerial and ground eavesdroppers. The links are considered to operate under the general κ-μ shadow channel fading model. To improve the secrecy performance efficiency, the GBS and UAV relays adopt beam-oriented communication while deploying safety zones around their expected accepting targets. Consequently, the almost exact closing expressions of the SOP are obtained under varied aerial and ground eavesdroppers' conditions. The SOP over Rayleigh fading as an extraordinary situation is also obtained. The simulation results demonstrated that UAV eavesdroppers impact the system performance more than ground eavesdroppers. Wu *et al.* [10] considered the impact of random UAV vibration interference and various non-colluding unintentional walk eavesdroppers on the security efficiency of the air-to-ground (A2G) eavesdropping system. Secrecy coverage probability (SCP) and ergodic secrecy capacity (ESC) expressions are acquired with features for the signal-to-noise ratio (SNR) received at legitimate receivers and eavesdroppers. Simulation results showed that UAV vibration interference can be employed to improve security efficiency of A2G eavesdropping system with applicable UAV height and beamwidth. In research [11]–[13], the study investigated UAV-assisted IoT communication systems operating in a completely incidental environment regarding the number of eavesdroppers and their positions around the earth source.

Moreover, to improve the system's security, we inspect the secrecy efficiency of the UAV IoT system with a favorable UAV that produces interference to confuse the eavesdroppers in [14]. By using stochastic geometry theory, the increasing allocation functions for the signal-to-noise plus-noise ratio of the main and eavesdropping links are obtained. After that, the analytical expressions of the SOP and the average secrecy rate (ASR) are achieved in [15], [16]. Ye *et al.* [17], [18] have studied UAVs and their rapid advancement to supply wider signal coverage and more comprehensive observation power in military and civil activities. The integration of UAVs into macrocellular networks is attracting remarkable attention to complement terrestrial cellular networks [19]–[21]. As an aerial base station, UAV is a progressive technology to supply wireless networks to users quickly. With the versatility and portability of UAVs, a major issue is how to better UAVs distribution to best meet immediately the needs of wireless network in a region. Azari *et al.* [22], Wang *et al.* [23], Wang *et al.* [24], Hayat *et al.* [25] have optimized the travel distance of the UAV in the selected area to optimize the average throughput and the probability of advantageous communication when the user density is low and the travel distance is small. The movement of the UAV becomes light when the user density is high.

In this paper, our main contributions can be outlined as follows: to look at the diversity performance of the considered network, we propose the system model and analytical expressions to indicate performance metrics such as the secrecy outage probability (SOP) and intercept probability (IP) of the proposed system, which is applicable to evaluate UAV-aided reliability.

The paper is organized as follows: section 2 describes the system model of mobile UAV-aided spatial distributions for secure communication. Section 3 provides for security performance analysis of ground users. Section 4 numerical results. Section 5 concludes of paper.

2. SYSTEM MODEL

As seen in Figure 1, we assume that the UAV is stationary and that the ground users (D) is placed in a circle, with O serving as the circle's center. More specifically, the ground users were deployed in the inner circle with a radius of R_1 meters to assess the users' performance at various distances from the UAV. Several randomly placed eavesdroppers (E) with the radius R_2 and R_1 meters were also deployed in the outer ring. The wireless connectivity between the UAV and the ground users is considered insignificant in the presence of natural or artificial impediments like trees or tall buildings. Thus, it is estimated that the UAV-to-D and UAV-to-E link follow the Rayleigh fading distributions, respectively. The homogeneous poisson point process (HPPP) model is used to simulate the geographic locations of the ground users and the listeners. We exploit homogeneous poisson point processes to model the locations of the users [26]. Hence, the ground users and eavesdroppers are uniformly distributed within their areas, and the probability density functions (PDF) of the distances from a user and eavesdroppers to the center are derived as Figure 1.

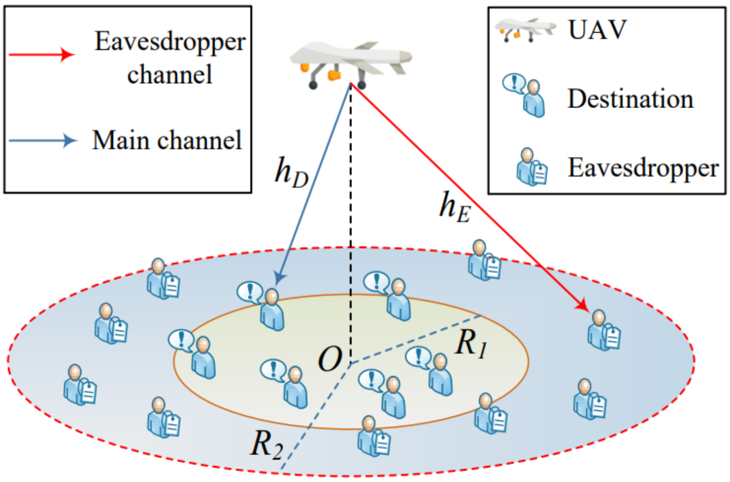

Figure 1. The system model of mobile UAV-aided spatial distributions for secure communication

$$f_{d_D}(x) = \frac{\partial}{\partial x}\frac{\pi x^2}{\pi R_1^2} = \frac{2x}{R_1^2}, \tag{1a}$$

$$f_{d_D}(x) = \frac{\partial}{\partial x}\frac{\pi x^2}{\pi R_1^2} = \frac{2x}{R_1^2}, \tag{1b}$$

First, UAVs receive signals and modify the signal, and forward them to ground users D and eavesdropper E. The received signals at both nodes are presented, respectively.

$$y_D = h_D\sqrt{\frac{P_{UAV}}{d_D^{\alpha}}}x_D + n_D, \tag{2a}$$

$$y_E = h_E\sqrt{\frac{P_E}{d_E^{\alpha}}}x_E + n_E, \tag{2b}$$

where h_D and h_E denote the Rayleigh fading channel between UAV-to-D and UAV-to-E. The channel power gains $|h_D|^2$ and $|h_E|^2$ are assumed to be exponentially distributed random variables (RVs) with the parameters λ_i, $i \in \{D, E\}$, respectively. P_{UAV} and P_E are the transmit power at the UAV and E, α refers to the path-loss factor while d_i indicates the distance between UAV-to-D link and UAV-to-E link, x_D and x_E are the superimposed signal vector satisfying the total power constraint $\mathbb{E}\{|x_D^2|^2\} = \mathbb{E}\{|x_E^2|^2\} = 1$ with $\mathbb{E}\{.\}$ is the expectation. n_i denotes the additive white Gaussian noise (AWGN) with $n_i \sim CN(0, N_0)$ in which $CN(a, b)$ complex normal distribution with average a and variance b.

In this scenario, the signal-to-noise-ratio (SNR) expressions of the ground users and eavesdroppers are presented as (3a) and (3b),

$$\Gamma_D = \frac{P_{UAV}|h_D|^2}{d_D^{\alpha}N_0} = \rho_U d_D^{-\alpha}|h_D|^2, \tag{3a}$$

$$\Gamma_E = \frac{P_E|h_E|^2}{d_E^{\alpha}N_0} = \rho_E d_E^{-\alpha}|h_E|^2, \tag{3b}$$

in which $\rho_U = \frac{P_{UAV}}{N_0}$ indicates the average SNR of the legal links between UAV and D, $\rho_E = \frac{P_E}{N_0}$ corresponds to the illegal link's average SNR between UAV and eavesdroppers E.

Assuming Rayleigh fading for both ground users and eavesdroppers, the probability density function (PDF) and cumulative distribution function (CDF) for channels are shown as (4a), (4b), (5a) and (5b).

$$f_{|h_E|^2}(x) = \frac{1}{\lambda_E} e^{-\frac{x}{\lambda_E}}, \tag{4a}$$

$$f_{|h_D|^2}(y) = \frac{1}{\lambda_D} e^{-\frac{y}{\lambda_D}}, \tag{4b}$$

and

$$F_{|h_E|^2}(x) = 1 - e^{-\frac{x}{\lambda_E}}, \tag{5a}$$

$$F_{|h_D|^2}(y) = 1 - e^{-\frac{y}{\lambda_D}}, \tag{5b}$$

where $\lambda_D = \mathbb{E}\{|h_D|^2\}$ and $\lambda_E = \mathbb{E}\{|h_E|^2\}$ are the corresponding channel variance.

3. SECURITY PERFORMANCE ANALYSIS

In this part, we analyze the secrecy performance for ground users' metrics using the SOP and IP expressions. With the analysis of SOP, by observing (8), it contains many RVs. Hence, the exact closed-form of SOP expression is very hard to obtain. By applying Gaussian-Chebyshev quadrature, the approximation SOP expression can be claimed while still assessing the physical significance of the system's characteristic parameters. The detailed analysis is given as follows.

3.1. SOP analysis

In this first analysis, the performance is an important metric to show the secure performance of the UAV-enabled system, the chance that the immediate secrecy capacity is less than the goal rate is known as the secure outage probability (SOP). Thus, channel capacities can be expressed as (6a) and (6b).

$$C_D = log_2\,(1 + \Gamma_D), \tag{6a}$$

$$C_E = log_2\,(1 + \Gamma_E). \tag{6b}$$

Then, the secrecy capacity can be (7a) and (7b).

$$C_{system} = max(C_D - C_E, 0). \tag{7}$$

The SOP is defined as the probability that secrecy capacity is below the secrecy rate threshold, thus SOP in the proposed system can be expressed as (8).

$$SOP_{system} = Pr\left(C_{system} < R_{th}\right) = 1 - Pr\left(\frac{1+\Gamma_D}{1+\Gamma_E} > 2^{R_{th}}\right) = 1 - Pr\left(|h_D|^2 > \frac{\vartheta d_D^\alpha}{d_E^\alpha}|h_E|^2 + \theta d_D^\alpha\right) \tag{8}$$

where R_{th} is so-called the secrecy rate threshold, $\vartheta = \frac{2^{R_{th}}\rho_E}{\rho_U}$ and $\theta = \frac{2^{R_{th}-1}}{\rho_U}$.

Lemma 1: The approximated secure outage probability of ground users closed-form statement is provided by (9).

$$SOP_{system} \approx 1 - \frac{\pi^3(R_2-R_1)}{2NKR_1^2(R_2^2-R_1^2)\lambda_E}\sum_{n=1}^{N}\sqrt{1-\phi_n^2}\sum_{k=1}^{K}\sqrt{1-\phi_k^2} \times sec^2\left(\frac{\pi(\phi_k+1)}{4}\right) e^{-\frac{\Theta(\phi_k)}{\lambda_E}} \Lambda(\phi_n) \frac{\gamma\left(\frac{2}{\alpha},\left(\frac{\vartheta\Theta(\phi_k)}{\lambda_D\Lambda(\phi_n)^\alpha}+\frac{\theta}{\lambda_D}\right)R_1^\alpha\right)}{\alpha\left(\frac{\vartheta\Theta(\phi_k)}{\lambda_D\Lambda(\phi_n)^\alpha}+\frac{\theta}{\lambda_D}\right)^{\frac{2}{\alpha}}}, \tag{9}$$

where $\Lambda(\phi_n) = \phi_n\left(\frac{R_2-R_1}{2}\right) + \left(\frac{R_2+R_1}{2}\right)$, $\phi_n = cos\left(\frac{2n-1}{2N}\pi\right)\$$, $\Theta(\phi_k) = tan\left(\frac{\pi(\phi_k+1)}{4}\right)$, $\phi_k = cos\left(\frac{2k-1}{2K}\pi\right)$, and $sec^2(x) = \frac{1}{cos^2(x)}$.

Proof: By definition, J denotes the complementary event at ground users and is calculated as (10).

$$J = Pr\left(|h_D|^2 > \frac{\vartheta d_D^\alpha}{d_E^\alpha}|h_E|^2 + \theta d_D^\alpha\right)$$
$$= \int_0^\infty f_{|h_E|^2}(x)\int_0^{R_1} f_{d_D}(r_1)\int_{R_1}^{R_2} f_{d_E}(r_2)\int_{\frac{\vartheta r_1^\alpha}{r_2^\alpha}x+\theta r_1^\alpha}^\infty f_{|h_D|^2}(y)\, dxdyd_{r_1}d_{r_2}. \quad (10)$$

Based on (4b), (4a), (1b) and (1a) into (10), J is written as (11).

$$J = \frac{4}{R_1^2(R_2^2-R_1^2)\lambda_D\lambda_E}\int_0^\infty e^{-\frac{x}{\lambda_E}}\int_0^{R_1} r_1\int_{R_1}^{R_2} r_2\int_{\frac{\vartheta r_1^\alpha}{r_2^\alpha}x+\theta r_1^\alpha}^\infty e^{-\frac{y}{\lambda_D}}\, dxdyd_{r_1}d_{r_2}$$
$$= \frac{4}{R_1^2(R_2^2-R_1^2)\lambda_E}\int_0^\infty e^{-\frac{x}{\lambda_E}}\int_0^{R_1} r_1\int_{R_1}^{R_2} r_2\, e^{-r_1^\alpha\left(\frac{\vartheta}{\lambda_D r_2^\alpha}x+\frac{\theta}{\lambda_D}\right)}dxd_{r_1}d_{r_2}. \quad (11)$$

Upon using [27], (3.381.3), the analytical expression of J is given by (12).

$$J = \frac{4}{R_1^2(R_2^2-R_1^2)\lambda_E}\int_0^\infty e^{-\frac{x}{\lambda_E}}\int_{R_1}^{R_2} r_2\frac{\gamma\left(\frac{2}{\alpha},\left(\frac{\vartheta}{\lambda_D r_2^\alpha}x+\frac{\theta}{\lambda_D}\right)R_1^\alpha\right)}{\alpha\left(\frac{\vartheta}{\lambda_D r_2^\alpha}x+\frac{\theta}{\lambda_D}\right)^{\frac{2}{\alpha}}}dxd_{r_2}. \quad (12)$$

Based on [28], we determined to obtain a closed-form formula J for the second integral to calculate and obtain an accurate approximation. Corresponding, we use Gaussian-Chebyshev quadrature [28], (25.4.38), J is written as (13).

$$J \approx \frac{2\pi(R_2-R_1)}{NR_1^2(R_2^2-R_1^2)\lambda_E}\sum_{n=1}^N\sqrt{1-\phi_n^2}\int_0^\infty e^{-\frac{x}{\lambda_E}}\Lambda(\phi_n)\frac{\gamma\left(\frac{2}{\alpha},\left(\frac{\vartheta}{\lambda_D\Lambda(\phi_n)^\alpha}x+\frac{\theta}{\lambda_D}\right)R_1^\alpha\right)}{\alpha\left(\frac{\vartheta}{\lambda_D\Lambda(\phi_n)^\alpha}x+\frac{\theta}{\lambda_D}\right)^{\frac{2}{\alpha}}}dx, \quad (13)$$

where

$$\Lambda(\phi_n) = \phi_n\left(\frac{R_2-R_1}{2}\right)+\left(\frac{R_2+R_1}{2}\right) \text{ and } \phi_n = cos\left(\frac{2n-1}{2N}\pi\right).$$

Let $t = \frac{4}{\pi}arctan(x)-1 \Rightarrow tan\left(\frac{\pi(t+1)}{4}\right) = x \Rightarrow \frac{\pi}{4}sec^2\left(\frac{\pi(t+1)}{4}\right)dt = dx$ and applying the Gaussian-Chebyshev quadrature, we have J is computed as (14).

$$J \approx \frac{\pi^2(R_2-R_1)}{2NR_1^2(R_2^2-R_1^2)\lambda_E}\sum_{n=1}^N\sqrt{1-\phi_n^2}\int_{-1}^1 \sec^2\left(\frac{\pi(t+1)}{4}\right)e^{-\frac{\Theta(t)}{\lambda_E}}$$
$$\times\Lambda(\phi_n)\frac{\gamma\left(\frac{2}{\alpha},\left(\frac{\vartheta\Theta(t)}{\lambda_D\Lambda(\phi_n)^\alpha}+\frac{\theta}{\lambda_D}\right)R_1^\alpha\right)}{\alpha\left(\frac{\vartheta\Theta(t)}{\lambda_D\Lambda(\phi_n)^\alpha}+\frac{\theta}{\lambda_D}\right)^{\frac{2}{\alpha}}}dt \approx \frac{\pi^3(R_2-R_1)}{2NKR_1^2(R_2^2-R_1^2)\lambda_E}\sum_{n=1}^N\sqrt{1-\phi_n^2}\sum_{k=1}^K\sqrt{1-\phi_k^2}$$
$$\times\sec^2\left(\frac{\pi(\phi_k+1)}{4}\right)e^{-\frac{\Theta(\phi_k)}{\lambda_E}}\Lambda(\phi_n)\frac{\gamma\left(\frac{2}{\alpha},\left(\frac{\vartheta\Theta(\phi_k)}{\lambda_D\Lambda(\phi_n)^\alpha}+\frac{\theta}{\lambda_D}\right)R_1^\alpha\right)}{\alpha\left(\frac{\vartheta\Theta(\phi_k)}{\lambda_D\Lambda(\phi_n)^\alpha}+\frac{\theta}{\lambda_D}\right)^{\frac{2}{\alpha}}}, \quad (14)$$

where $sec^2(x) = \frac{1}{cos^2(x)}$, $\Theta(\phi_k) = tan\left(\frac{\pi(\phi_k+1)}{4}\right)$ and $\phi_k = cos\left(\frac{2k-1}{2K}\pi\right)$. Substituting (14) into (8), (9) can be obtained and the proof is completed.

3.2. Intercept probability analysis

In this second analysis, we examine the UAV system's performance regarding IP secrecy in the presence of randomly placed ground users. The IP will be occurred if and only if the information from x_D is accurately decoded at the ground users and the eavesdropper will be able to intercept the information of the ground users successfully.

Based on above description, user *D* will be intercepted if *E* can successfully wiretap *J*'s signal. Then, the *IP* of *D* by *E* is shown as (15).

$$IP_{system} = Pr(C_D > R_{th}, C_E > R_{th}) = Pr(|h_D|^2 > d_D^\alpha \zeta_D, |h_E|^2 > d_E^\alpha \zeta_E), \tag{15}$$

where $\zeta_D = \frac{2^{R_{th}-1}}{\rho_U}$ and $\zeta_E = \frac{2^{R_{th}-1}}{\rho_E}$.

Lemma 2: The precise closed-form equation for the *IP* of *D* for Rayleigh fading channels is provided by (16).

$$IP_{system} = \frac{4\lambda_D^{\frac{2}{\alpha}}\lambda_E^{\frac{2}{\alpha}}}{\alpha^2 R_1^2 (R_2^2 - R_1^2)\zeta_D^{\frac{2}{\alpha}}\zeta_E^{\frac{2}{\alpha}}} \gamma\left(\frac{2}{\alpha}, \frac{\zeta_D}{\lambda_D} R_1^\alpha\right)\left[\gamma\left(\frac{2}{\alpha}, \frac{\zeta_E}{\lambda_E}\right) + \Gamma\left(\frac{2}{\alpha}, \frac{\zeta_E}{\lambda_E}\right)\right.$$
$$\left. -\Gamma\left(\frac{2}{\alpha}, \frac{\zeta_E}{\lambda_E} R_2^\alpha\right) - \gamma\left(\frac{2}{\alpha}, \frac{\zeta_E}{\lambda_E} R_1^\alpha\right)\right], \tag{16}$$

where $\gamma(.,.)$ is the lower incomplete Gamma function and $\Gamma(.,.)$ is the upper incomplete Gamma function.
Proof: We have intercept probability calculated as (17).

$$IP_{system} = \frac{4}{R_1^2(R_2^2 - R_1^2)} \int_0^{R_1} x e^{-\frac{\zeta_D x^\alpha}{\lambda_D}} \int_{R_1}^{R_2} y e^{-\frac{\zeta_E y^\alpha}{\lambda_E}} dxdy$$
$$= \frac{4}{R_1^2(R_2^2 - R_1^2)} \int_0^{R_1} x e^{-\frac{\zeta_D x^\alpha}{\lambda_D}} dx \left[\int_0^\infty y e^{-\frac{\zeta_E y^\alpha}{\lambda_E}} dy - \int_{R_2}^\infty y e^{-\frac{\zeta_E y^\alpha}{\lambda_E}} dy - \int_0^{R_1} y e^{-\frac{\zeta_E y^\alpha}{\lambda_E}} dy\right]. \tag{17}$$

where we have used [27], (3.381.8), [27], (3.381.9) and [27], (3.381.10) to solve the corresponding integral. In order to do this, a few straightforward mathematical operations may be used to quickly arrive at the required Lemma 2 outcome.

4. MUMERICAL RESULTS

In this part, we demonstrate the outage performance by numerically simulating various theoretical findings from some figures. The primary system parameters are set at $R_1 = 5$ m, $R_2 = 20$ m, $R_{th} = 1$, $\rho_E = 10$ dB, $\lambda_D = 1$ and $\lambda_E = 1$. Additionally, data from a Monte-Carlo simulation run 10^6 times are given to confirm our analytical findings. In the following figures, we denote "Exact theory" and "Simulation" as analytical computation and Monte-Carlo computation-based simulations, respectively. In addition, the Gauss-Chebyshev parameter is selected as *N*=*K*=200 to earn the closest result.

We provide the SOP curves for various values as shown in subsection 3.1, when ρ_E is big, the SOP of the system alters, as can be seen in Figure 2. The SOP performance in this scenario solely pertains to ρ_U and ρ_E. However, since the superimposed message is transmitted to two different destinations, the systems have a higher security requirement than conventional point-to-point communication, so small values for the target rate and the average SNR of the eavesdropper link should be chosen in order to ensure reliable communication.

In Figure 3, the random ground users and random eavesdropper selection are plotted. We can see that when the rate of radius R_1 grows, the outage of the ground users happens more frequently. This is due to the fact that in our suggested protocol, higher outages might occur when the user decodes the signal themselves, yet the radius is close to the eavesdropper. As a result, extending the radius R_1 makes it more difficult to decode, which will result in more outages. A crucial finding is that choosing the wrong radius R_1 will result in an outage probability of one.

The SOP vs. target rate for various fading parameters ($\rho_U = 10; 30; 40$ dB) and ($\rho_E = 10; 20$ dB) is shown in Figure 4 under ideal circumstances. We can observe from Figure 4 that when R_{th} grows, the ground users SOP also rises. The dependability of the system under consideration rises together with the average SNR of the illicit link, increasing SOP.

For various transmit SNR levels, Figure 5 shows the IP vs. the target rate. The IP of SNR=25 dB is superior to SNR=20 dB, SNR=15 dB, and SNR=10 dB, as can be shown. Additionally, we can see that the target rate has a significant influence on the ground users.

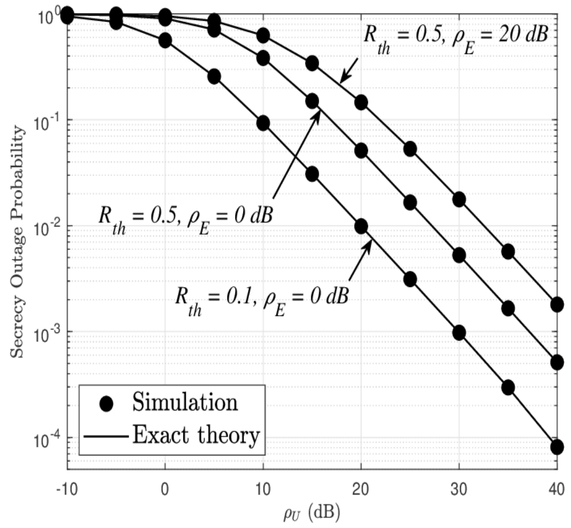

Figure 2. SOP versus ρ_U for different secrecy SNR taget data values

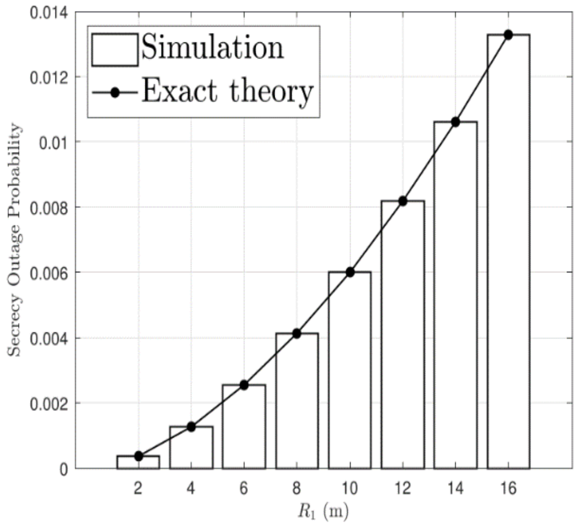

Figure 3. SOP of the ground users versus radius with R_1, where $R_2 = 20$ m, $\rho_E = 10$ dB and $\rho_U = 30$ dB

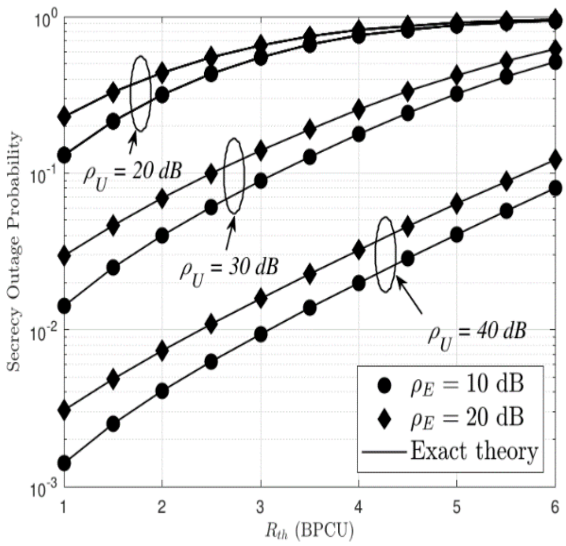

Figure 4. SOP versus the target rate (R_{th}) for ρ_U

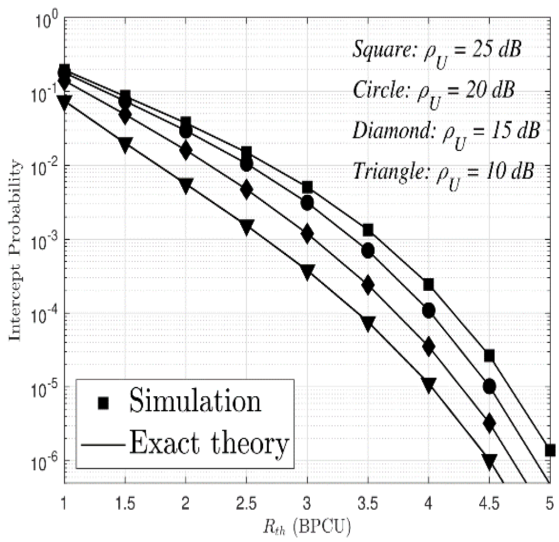

Figure 5. IP versus the target rate (R_{th}) for ρ_U

5. CONCLUSION

In this paper, we considered the domain of wireless communication systems in which UAVs can serve ground users. The security of wireless networks is a serious aspect of the system's performance and reliability. We have focused on security issues and mitigation techniques for the outage of the ground users in wireless with SOP and IP parameters of the system. Furthermore, all analytical results are verified by Monte Carlo simulations. Based on the analysis in the paper, we can extend to the generic framework of the UAVs mobility application to examine the efficiency of a more significant number of NOMA users in future work.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviews for the helpful comments and suggestions. This work is a part of the basic science research program CSA2021-10 funded by Saigon University. The research leading to these results was supported by Czech Ministry of Education, Youth and Sports under project reg. no. SP2021/25 and partially under the e-INFRA CZ project ID:90140.

REFERENCES

[1] 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. 112858–112897, 2022, doi: 10.1109/ACCESS.2022.3215975.

[2] A. Z. Md. Imran, M. L. Hakim, M. R. Ahmed, M. T. Islam, and E. Hossain, “Design of microstrip patch antenna to deploy unmanned aerial vehicle as UE in 5G wireless network,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4202–4213, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4202-4213.

[3] C.-B. Le and D.-T. Do, “Employing non-orthogonal multiple access scheme in UAV-based wireless networks,” *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 10, no. 1, pp. 241–248, Feb. 2021, doi: 10.11591/eei.v10i1.2102.

[4] N.-T. Nguyen, H.-N. Nguyen, L. T. Huynh, and M. Voznak, “Enabling unmanned aerial vehicle to serve ground users in downlink NOMA system,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 6, pp. 3338–3345, Dec. 2022, doi: 10.11591/eei.v11i6.3945.

[5] B. Ji, Y. Li, S. Chen, C. Han, C. Li, and H. Wen, “Secrecy outage analysis of UAV assisted relay and antenna selection for cognitive network Under nakagami- m channel,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 3, pp. 904–914, Sep. 2020, doi: 10.1109/TCCN.2020.2965945.

[6] B. Ji, Y. Li, D. Cao, C. Li, S. Mumtaz, and D. Wang, “Secrecy performance analysis of UAV assisted relay transmission for cognitive network with energy harvesting,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7404–7415, Jul. 2020, doi: 10.1109/TVT.2020.2989297.

[7] M. Li, X. Tao, N. Li, H. Wu, and J. Xu, “Secrecy energy efficiency maximization in UAV-enabled wireless sensor networks without eavesdropper’s CSI,” *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3346–3358, Mar. 2022, doi: 10.1109/JIOT.2021.3098049.

[8] H. Liu, S.-J. Yoo, and K. S. Kwak, “Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers,” *Journal of Communications and Networks*, vol. 20, no. 5, pp. 496–508, Oct. 2018, doi: 10.1109/JCN.2018.000074.

[9] T. Bao, H. Wang, W.-J. Wang, H.-C. Yang, and M. Hasna, “Secrecy outage performance analysis of UAV-assisted relay communication systems with multiple aerial and ground eavesdroppers,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 3, pp. 2592–2600, Jun. 2022, doi: 10.1109/TAES.2021.3131631.

[10] H. Wu, H. Li, Z. Wei, N. Zhang, and X. Tao, “Secrecy performance analysis of air-to-ground communication with UAV jitter and multiple random walking eavesdroppers,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 572–584, Jan. 2021, doi: 10.1109/TVT.2020.3047082.

[11] H. Lei *et al.*, “Safeguarding UAV IoT communication systems against randomly located eavesdroppers,” *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1230–1244, Feb. 2020, doi: 10.1109/JIOT.2019.2953903.

[12] Z. Xiang, X. Tong, and Y. Cai, “Secure transmission for NOMA systems with imperfect SIC,” *China Communications*, vol. 17, no. 11, pp. 67–78, Nov. 2020, doi: 10.23919/JCC.2020.11.006.

[13] T. Wu, Y. Zou, and Y. Jiang, “Secrecy throughput optimization and precoding design in adaptive transmit antenna selection systems with limited feedback,” *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 11693–11702, Nov. 2022, doi: 10.1109/TVT.2022.3190681.

[14] V.-H. Dang *et al.*, “Throughput optimization for NOMA energy harvesting cognitive radio with multi-UAV-assisted relaying under security constraints,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 1, pp. 82–98, Feb. 2023, doi: 10.1109/TCCN.2022.3225165.

[15] J. Tang, G. Chen, and J. P. Coon, “Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 3026–3041, Nov. 2019, doi: 10.1109/TIFS.2019.2912074.

[16] W. Wang, H. Tian, and W. Ni, “Secrecy performance analysis of IRS-aided UAV relay system,” *IEEE Wireless Communications Letters*, vol. 10, no. 12, pp. 2693–2697, Dec. 2021, doi: 10.1109/LWC.2021.3112752.

[17] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, “Secure UAV-to-UAV systems with spatially random UAVs,” *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 564–567, Apr. 2019, doi: 10.1109/LWC.2018.2879842.

[18] D. Kim, J. Lee, and T. Q. S. Quek, “Multi-layer unmanned aerial vehicle networks: Modeling and performance analysis,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 325–339, Jan. 2020, doi: 10.1109/TWC.2019.2944378.

[19] J. Ye, S. Dang, B. Shihada, and M.-S. Alouini, “Space-air-ground integrated networks: Outage performance analysis,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 7897–7912, Dec. 2020, doi: 10.1109/TWC.2020.3017170.

[20] B. Li, Z. Fei, Y. Zhang, and M. Guizani, “Secure UAV communication networks over 5G,” *IEEE Wireless Communications*, vol. 26, no. 5, pp. 114–120, Oct. 2019, doi: 10.1109/MWC.2019.1800458.

[21] S. Jia and L. Zhang, “Modelling unmanned aerial vehicles base station in ground-to-air cooperative networks,” *IET Communications*, vol. 11, no. 8, pp. 1187–1194, Jun. 2017, doi: 10.1049/iet-com.2016.0808.

[22] M. M. Azari, F. Rosas, K.-C. Chen, and S. Pollin, “Ultra reliable UAV communication using altitude and cooperation diversity,” *IEEE Transactions on Communications*, vol. 66, no. 1, pp. 330–344, Jan. 2018, doi: 10.1109/TCOMM.2017.2746105.

[23] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, “Survey on unmanned aerial vehicle networks: A cyber physical system perspective,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1027–1070, 2020, doi: 10.1109/COMST.2019.2962207.

[24] Z. Wang, L. Duan, and R. Zhang, “Adaptive deployment for UAV-aided communication networks,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 9, pp. 4531–4543, Sep. 2019, doi: 10.1109/TWC.2019.2926279.

[25] S. Hayat, E. Yanmaz, and R. Muzaffar, “Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2624–2661, 2016, doi: 10.1109/COMST.2016.2560343.

[26] J. Andrews, R. Ganti, M. Haenggi, N. Jindal, and S. Weber, “A primer on spatial modeling and analysis in wireless networks,” *IEEE Communications Magazine*, vol. 48, no. 11, pp. 156–163, Nov. 2010, doi: 10.1109/MCOM.2010.5621983.

[27] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. 6th ed. New York, NY, USA: Academic Press, 2015.

[28] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. New York, NY, USA: Dover Publications; 0009-Revised edition, 1965.

BIOGRAPHIES OF AUTHORS

Cuu Ho Van received the B.S. degree in telecommunication engineering in 1987 and the M.S. degree in telecommunication engineering in 1997 from Hanoi University of Science and Technology, Vietnam. In 2006 he is degrees Ph.D. in communication technology at Posts and Telecommunications Institute of Technology. He is currently a lecturer at the Faculty of Electronics and Telecommunications (FET) at Saigon University, Ho Chi Minh City, Vietnam. His research interest includes wireless communication in 5G, data communication, and networks. He can be contacted at email: cuuhovan@sgu.edu.vn.

Hong-Nhu Nguyen received a B.Sc. in Electronics Engineering from Ho Chi Minh city University of Technology in 1998 and an M.Sc. in Electronics Engineering from the University of Transport and Communications (Vietnam) in 2012. He is currently working as lecturer at Saigon University, Ho Chi Minh City, Vietnam. He received his Ph.D. in telecommunication from Technical University of Ostrava, Czech Republic in 2021. His research interest includes applied electronics, wireless communications, cognitive radio, NOMA and energy harvesting. He can be contacted at email: nhu.nh@sgu.edu.vn.

Si-Phu Le was born in Da Nang city, Vietnam, in 1985. He received a B.Sc. from Nha Trang University, Nha Trang, Vietnam in 2008 and an M.B.A. from Open University of Malaysia in 2013. He was lecturer in the IT Department of Van Lang University from 2009 to 2020. He is currently working as Managing Director at ACEXIS JSC. His research interests include electronic design, digital signal processing, MINO, and intelligent reflecting surfaces. He is studying PhD in Telecommunication from Technical University of Ostrava, Czech Republic in 2023. He can be contacted at email: phu.le.si.st@vsb.cz.

Miroslav Voznak (M'09-SM'16) received his Ph.D. in telecommunications in 2002 from the Faculty of Electrical Engineering and Computer Science at VSB-Technical University of Ostrava and achieved habilitation in 2009. He was appointed full professor in Electronics and Communications Technologies in 2017. His research interests generally focus on ICT, especially on quality of service and experience, network security, wireless networks, and big data analytics. He has authored and co-authored over one hundred articles in SCI/SCIE journals. According to the Stanford University study released in 2020, he is one of the world's top 2% of scientists in networking and telecommunications and information and communications technologies. He served as a general chair of the 11th IFIP Wireless and Mobile Networking Conference in 2018 and the 24th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications in 2020. He participated in six projects funded by the EU in programs managed directly by the European Commission. Currently, he is a principal investigator in the research project QUANTUM5 funded by NATO, which focuses on the application of quantum cryptography in 5G campus networks. He can be contacted at email: miroslav.voznak@vsb.cz.