Received 22 August 2023; revised 7 September 2023; accepted 13 September 2023. Date of publication 19 September 2023;
date of current version 30 November 2023.

Digital Object Identifier 10.1109/OJCOMS.2023.3316919

Secrecy Analysis of Directional mmWave UAV-Based Links Under Hovering Fluctuations

SAUD ALTHUNIBAT [1,3] (Senior Member, IEEE), MOHAMMAD TAGHI DABIRI [2], MAZEN O. HASNA [2] (Senior Member, IEEE), AND KHALID QARAQE [3] (Senior Member, IEEE)

[1] Department of Communications Engineering, Al-Hussein Bin Talal University, Ma'an 71111, Jordan

[2] Department of Electrical Engineering, Qatar University, Doha, Qatar

[3] Department of Electrical and Computer Engineering, Texas A&M University at Qatar, Doha, Qatar

CORRESPONDING AUTHOR: S. ALTHUNIBAT (e-mail: saud.althunibat@ahu.edu.jo)

This publication was made possible by NPRP14C-0909-210008 from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the author[s].

ABSTRACT Recent developments in Unmanned Aerial Vehicles (UAVs) technology have paved the way to their utilization in different fields and applications. Among these applications, UAVs have been widely investigated as a good candidate to serve as mobile base-stations that can provide prompt and temporary coverage of wireless connectivity for specific areas. Recent studies that address different UAVs' performance aspect lack of considering more practical channel models. Therefore, in this paper, based on a recent three dimensional channel modeling of UAV-based links, the secrecy analysis is in detail conducted for UAV-based links operating on the millimeter wave band. Specifically, the average channel capacity, the average secrecy capacity and the probability of strictly positive secrecy capacity are all investigated between two UAVs in the presence of another UAV-based eavesdropper. Our results include closed form expressions of the addressed secrecy metrics along with simulation results that reveal the impact of different operational parameters on the secrecy performance.

INDEX TERMS Secrecy capacity, secrecy analysis, unmanned aerial vehicles, millimeter wave, hovering fluctuations, directional antennas.

I. INTRODUCTION

In EMERGENCY cases, such as natural disasters and military attacks, maintaining wireless connectivity is a main concern for local authorities. This is mainly due to the expected damage that might affect the terrestrial communications infrastructure, which limits the situation awareness and the rescue efforts that are essential in emergency management. Therefore, it is of paramount importance for local authorities to consider preparing a prompt, reliable and efficient spare network for such scenarios. To this end, Unmanned Aerial Vehicles (UAVs) have been widely proposed as an efficient solution to replace the damaged infrastructure and provide the required wireless connectivity [1], [2].

Compared to terrestrial systems, UAV-based communication systems are usually faster to deploy, more flexible and more cost efficient [3], which makes them promising candidate for emergency scenarios [4], [5]. The employment and operation of UAV-based links are not trivial where several challenges have been reported, which may impact their achievable performance [6]. These challenges include three dimensional UAV deployment, trajectory optimization, channel modeling, performance analysis, and resource management [4]. Although these challenges are present in traditional terrestrial systems, however, when dealing with mobile aerial entities, such issues become more critical and have a significant impact on the overall performance. Therefore, recent literature has intensively addressed these challenges. For instance, in [7], the characterization of the air-to-ground channel is addressed focusing on delay spread, path loss and multipath fading. In [8], the path loss is modeled for high altitude air-to-ground link. The study in [9] reveals that proper deployment of UAVs can lead to improved channel quality as compared to ground base stations. Recently, 3D channel modeling for UAV-to-UAV has been investigated for millimeter wave links in [10] and for free space optical links in [11]. In both works, the fluctuations of the UAVs have been considered due to their impact on both the position and orientation of the link. Differently, optimizing the mobility of multiple UAVs was addressed in [12] considering data gathering from IoT nodes. In [13], maximizing the coverage area by optimizing the altitude of the UAV is investigated. Another set of works have analyzed the different performance aspects of UAV-based systems including coverage probability for ground user served by multiple UAVs [14], outage probability and error rate for a single UAV-based link [15], rate performance of a single UAV [16], Signal-to-Noise Ratio (SNR) distribution and capacity analysis for UAV-ground links [17], throughput analysis for UAV-based relay in cellular networks [18].

Aiming at complementing the research efforts in analyzing performance of the UAV-based links, this work addresses the secrecy analysis as one of the main performance aspects. To the best of our knowledge, only few works have investigated the secrecy analysis in UAV-based links based on practical channel modelling [19]. For example, in [20], a UAV is utilized as a jammer to enhance the secrecy capacity between two ground users. Likewise in [21], the jamming signal generated from the UAV is utilized to protect the IoT ground users communicating with a hovering UAV. In [22], the secrecy performance is analyzed for Reconfigurable Intelligent Surface (RIS)-aided communication link in the presence of multiple eavesdropping UAVs. In [23], the maximization of secure energy efficiency is investigated for RIS-equipped UAV that is acting as a relay for ground users. The maximization problem is solved by optimizing the trajectory, the phase shift of the RIS and transmit power. Results in [24] reveal that an aerial eavesdropper can be a serious threat for ground-ground link, where the secrecy rate is shown to be very small. Considering a different setup in [25], the secrecy rate is investigated for the link between a UAV and a ground receiver in the presence of a ground eavesdropper, where a joint trajectory and transmit power optimization is conducted to maximize the secrecy rate. Similarly in [26], the secrecy performance is analyzed for the same setup considered in [25] except that the UAV jitter is taken into account. More related to our work, the secrecy analysis is investigated in [27] for a UAV-UAV link considering the presence of multiple eavesdropping UAVs. The locations of all UAVs (including legitimate and eavesdroppers UAVs) are randomly distributed according to stochastic geometry. Both secrecy outage probability and average secrecy capacity have been derived in closed form expressions. However, the channels are modeled considering only free space path loss model without taking fading and shadowing into account. Such an assumption may hold for the lower RF band, while it might be inapplicable for higher bands such as Millimeter wave (mmWave) band [28].

TABLE 1. The list of main notations.

Parameter	Description
$\mathcal{A}$	Denote Alice
$\mathcal{B}$	Denote Bob
$\mathcal{E}$	Denote Eve
$\phi_{\mathcal{E}}$	Eve's angle relative to the main link shown in Fig. 1
$Z_{\mathcal{AB}}$	Link length between $\mathcal{A}$ and $\mathcal{B}$
$Z_{\mathcal{AE}}$	Link length between $\mathcal{A}$ and $\mathcal{E}$
$N_{\mathcal{A}} \times N_{\mathcal{A}}$	Number of antenna elements of $\mathcal{A}$
$N_{\mathcal{B}} \times N_{\mathcal{B}}$	Number of antenna elements of $\mathcal{B}$
$N_{\mathcal{E}} \times N_{\mathcal{E}}$	Number of antenna elements of $\mathcal{E}$
$\theta_{\mathcal{A}}$	Defined in (1) which is a function of $\theta_{\mathcal{A}x}$ and $\theta_{\mathcal{A}y}$
$\theta_{\mathcal{B}}$	Defined in (1) which is a function of $\theta_{\mathcal{B}x}$ and $\theta_{\mathcal{B}y}$
$\theta_{\mathcal{E}}$	Defined in (1) which is a function of $\theta_{\mathcal{E}x}$ and $\theta_{\mathcal{E}y}$
$\theta_{\mathcal{A}_x}$	Instantaneous fluctuations of $\mathcal{A}$ in the direction pf x axis with distribution $\sim \mathcal{N}\{\theta'_{\mathcal{A}_x}, \sigma^2_{\theta_{\mathcal{A}}}\}$
$\theta_{\mathcal{A}_y}$	Instantaneous fluctuations of $\mathcal{A}$ in the direction pf y axis with distribution $\sim \mathcal{N}\{\theta'_{\mathcal{A}_y}, \sigma^2_{\theta_{\mathcal{A}}}\}$
$\theta_{\mathcal{B}_x}$	Instantaneous fluctuations of $\mathcal{B}$ in the direction pf x axis with distribution $\sim \mathcal{N}\{\theta'_{\mathcal{B}_x}, \sigma^2_{\theta_{\mathcal{B}}}\}$
$\theta_{\mathcal{B}_y}$	Instantaneous fluctuations of $\mathcal{B}$ in the direction pf y axis with distribution $\sim \mathcal{N}\{\theta'_{\mathcal{B}_y}, \sigma^2_{\theta_{\mathcal{B}}}\}$
$\theta_{\mathcal{E}_x}$	Instantaneous fluctuations of $\mathcal{E}$ in the direction pf x axis with distribution $\sim \mathcal{N}\{\theta'_{\mathcal{E}_x}, \sigma^2_{\theta_{\mathcal{E}}}\}$
$\theta_{\mathcal{E}_y}$	Instantaneous fluctuations of $\mathcal{E}$ in the direction pf y axis with distribution $\sim \mathcal{N}\{\theta'_{\mathcal{E}_y}, \sigma^2_{\theta_{\mathcal{E}}}\}$

Different from the aforementioned approaches, in this paper, we consider a unique setup of the UAV-based link where the transmitter, the receiver, and the eavesdropper are aerial entities. Moreover, the channel model considered in this paper takes into account the vibration of the UAVs and its impact on the mmWave link adopted. Actually, the vibration of the UAV due to the mobility of its internal mechanical parts or the wind impact will definitely affect the orientation of the UAV, which represents a serious challenge for transmitters/receivers operating over mmWave bands that are sensitive to alignment errors [29]. The contribution of this work is summarized as follows.

- First, we characterize the tackled communication system by considering the actual 3D antenna patterns, the intensity of UAVs' instabilities and their effect on antenna misalignment, and the position of the eavesdropper with respect to the legal transmitter and receivers.
- Second, the secrecy analysis is addressed by evaluating the average channel capacity, the average secrecy capacity, and the probability of strictly positive secrecy capacity.
- Third, mathematical closed-from expressions are derived for the three performance metrics along with an investigation of the impact of different operational parameters on them.
- Finally, using simulation, we deal with the performance of important parameters on the secrecy metrics. We examine the relationship between the secrecy capacity and stability of the UAV link. We also show how by optimally choosing the antenna pattern, you can place the eavesdropper on the sub-lobes of the antenna and increase the secrecy capacity.

The rest of the paper is organized as follows. Section II describes the system model along with the different specifications and assumptions adopted for both legitimate UAVs and the eavesdropping UAV. The secrecy analysis is conducted in Section III that details the mathematical framework followed to derive the secrecy metrics considered. In Section IV, simulation and analytical results are presented along with the sufficient discussion. Finally, in Section V, conclusions are drawn and the plan for future work is presented.

II. SYSTEM MODEL

The adopted system model in this paper, depicted in Fig. 1, includes three different aerial entities; the transmitter Alice, denoted by $\mathcal{A}$, the legitimate receiver Bob, denoted by $\mathcal{B}$, and the eavesdropper, denoted by $\mathcal{E}$. It is considered that the three entities are based on hovering UAVs. Also, it is assumed that $\mathcal{A}$ transmits data towards $\mathcal{B}$ over the mmWave band using directional antennas, while $\mathcal{E}$ is eavesdropping the link between $\mathcal{A}$ and $\mathcal{B}$ aiming to reveal the transmitted data. As known, a hovering UAV will be vibrating due to either its internal mechanical vibration or external wind impact. Such a vibration will definitely lead to fluctuation in both the position and orientation of both $\mathcal{A}$ and $\mathcal{B}$. Therefore, as directional mmWave/THz links are sensitive to such fluctuations of both $\mathcal{A}$ and $\mathcal{B}$, their impact on the link's performance should be taken into account. Fig. 1 depicts the system 3D model, where the average locations of $\mathcal{A}$ and $\mathcal{B}$ are considered at the points $(0, 0, 0)$ and $(0, 0, Z_{\mathcal{AB}})$ where $Z_{\mathcal{AB}}$ represents the spacing distance between $\mathcal{A}$ and $\mathcal{B}$. The UAV's fluctuations deviate both Angel of Departure (AoD) at $\mathcal{A}$ and Angle of Arrival (AoA) at $\mathcal{B}$ in the planes $x - z$ and $y - z$, which are denoted by the angles $\theta_{\mathcal{A}} = (\theta_{\mathcal{A}x}, \theta_{\mathcal{A}y})$, respectively, for $\mathcal{A}$ and by $\theta_{\mathcal{B}} = (\theta_{\mathcal{B}x}, \theta_{\mathcal{B}y})$ for $\mathcal{B}$. Based on the results of [10], [30], [31], UAV's vibrations can be well modeled as $\theta_{\mathcal{A}_x} \sim \mathcal{N}\{\theta'_{\mathcal{A}_x}, \sigma^2_{\theta_{\mathcal{A}}}\}$, $\theta_{\mathcal{A}_y} \sim \mathcal{N}\{\theta'_{\mathcal{A}_y}, \sigma^2_{\theta_{\mathcal{A}}}\}$, $\theta_{\mathcal{B}_x} \sim \mathcal{N}\{\theta'_{\mathcal{B}_x}, \sigma^2_{\theta_{\mathcal{B}}}\}$, and $\theta_{\mathcal{B}_y} \sim \mathcal{N}\{\theta'_{\mathcal{B}_y}, \sigma^2_{\theta_{\mathcal{B}}}\}$.

Both $\mathcal{A}$ and $\mathcal{B}$ are equipped by a single identical antenna that is considered to be uniform square array antenna. The considered antenna consists of $N \times N$ that are spaced by r in both x and y dimensions. The gain of the array radiation of $\mathcal{A}$ is expressed in terms of two angles, namely, $\theta_{\mathcal{A}}$ and $\Phi_{\mathcal{A}}$ that are defined as follows

$$\theta_{\mathcal{A}} = \arctan\left(\sqrt{\tan^2(\theta_{\mathcal{A}x}) + \tan^2\big(\theta_{\mathcal{A}y}\big)}\right), \tag{1}$$

and

$$\Phi_{\mathcal{A}} = \arctan\left(\frac{\tan\big(\theta_{\mathcal{A}y}\big)}{\tan(\theta_{\mathcal{A}x})}\right), \tag{2}$$

which can both contribute in the gain as follows

$$G_{\mathcal{A}} = G_0 G_e G_a, \tag{3}$$

where G_e is the radiation pattern of a single antenna element, G_a is the array factor, and G_0 is defined in (10). G_e is defined in 3GPP as follows

$$G_e = 10^{\frac{G_{e,3\text{dB}}}{10}}, \tag{4}$$

where $G_{e,3\text{dB}}$ is defined as [32]

$$G_{e,3\text{dB}} = G_{max} - \min\big\{-\big(G_{e,3\text{dB},1} + G_{e,3\text{dB},2}\big), F_m\big\}, \tag{5}$$

$$G_{e,3\text{dB},1} = -\min\left\{12\left(\frac{\theta_e - 90}{\theta_{e3\text{dB}}}\right)^2, G_{SL}\right\}, \tag{6}$$

$$G_{e,3\text{dB},2} = -\min\left\{12\left(\frac{\theta_{\mathcal{A}x}}{\phi_{e3\text{dB}}}\right)^2, F_m\right\}, \tag{7}$$

$$\theta_e = \arctan\left(\frac{\sqrt{1 + \sin^2(\theta_{\mathcal{A}x})}}{\sin\big(\theta_{\mathcal{A}y}\big)}\right), \tag{8}$$

where G_{max} is the maximum directional gain of the antenna element set to $G_{max} = 8\text{dBi}$, F_m represents the front-back ratio set to $F_m = 30$, G_{SL} is the side-lobe level limit set to $G_{SL} = 30$, and $\theta_{e3\text{dB}} = 65^o$ and $\phi_{e3\text{dB}} = 65^o$ represent the vertical and horizontal 3D beamwidths, respectively. The array factor G_a for a square array $N_{\mathcal{A}} \times N_{\mathcal{A}}$ is given as follows [33, eqs. (6.89) and (6.91)]:

$$G_a = \left(\frac{\sin\big(N_{\mathcal{A}}\frac{\pi}{2}\sin(\theta_{\mathcal{A}})\cos(\Phi_{\mathcal{A}})\big)}{N_{\mathcal{A}}\sin\big(\frac{\pi}{2}\sin(\theta_{\mathcal{A}})\cos(\Phi_{\mathcal{A}})\big)}\right)^2 \times \left(\frac{\sin\big(N_{\mathcal{A}}\frac{\pi}{2}\sin(\theta_{\mathcal{A}})\sin(\Phi_{\mathcal{A}})\big)}{N_{\mathcal{A}}\sin\big(\frac{\pi}{2}\sin(\theta_{\mathcal{A}})\sin(\Phi_{\mathcal{A}})\big)}\right)^2, \tag{9}$$

where the progressive phase shifts are set to zero for the x and y directions, and the spacing between the elements is set to $\frac{\lambda}{2}$ in both directions. Finally, G_0 is determined as follows [33]

$$G_0 = \frac{1}{\int_o^{\pi}\int_0^{2\pi} G_e G_a \sin(\theta_{\mathcal{A}}) d\theta_{\mathcal{A}} d\Phi_{\mathcal{A}}}. \tag{10}$$

The antenna gain of $\mathcal{B}$, i.e., $G_{\mathcal{B}}$, can be expressed in a similar way to $G_{\mathcal{A}}$, $N_{\mathcal{A}}$ and replacing $\theta_{\mathcal{A}}$, $\Phi_{\mathcal{A}}$, $\theta_{\mathcal{A}x}$ and $\theta_{\mathcal{A}y}$ by $\theta_{\mathcal{B}}$, $\Phi_{\mathcal{B}}$, $\theta_{\mathcal{B}x}$, $N_{\mathcal{B}}$ and $\theta_{\mathcal{B}y}$, respectively, with all assumptions used in formulating $G_{\mathcal{A}}$.

Accordingly, the instantaneous SNR of the $\mathcal{A} - \mathcal{B}$ at $\mathcal{B}$'s end, denoted by γ_1 can be expressed as follows

$$\gamma_1 = \frac{P|h|^2 L_{\mathcal{AB}} \mathbb{G}_{\mathcal{AB}}}{\sigma^2}, \tag{11}$$

where $\mathbb{G}_{\mathcal{AB}} = G_{\mathcal{A}} G_{\mathcal{B}}$, P is the transmit power, $L_{\mathcal{AB}}$ is the path loss, h is the coefficient of the small-scale fading and σ^2 is the noise power. The path loss $L_{\mathcal{AB}}$ mainly depends on the distance $Z_{\mathcal{AB}}$ and has been reported in 3GPP recent report as follows [34]

$$L_{\mathcal{AB}} = -20\log\left(\frac{40\pi Z_{\mathcal{AB}} f_c}{3}\right) + \min\left\{0.044T^{1.73}, 14.77\right\} + \min\left\{0.03T^{1.73}, 10\right\}\log(Z_{\mathcal{AB}}) - 0.002 Z_{\mathcal{AB}}\log_{10}(T), \tag{12}$$

where T represents the average building height in meters. Finally, the fading model usually adopted for low-altitude

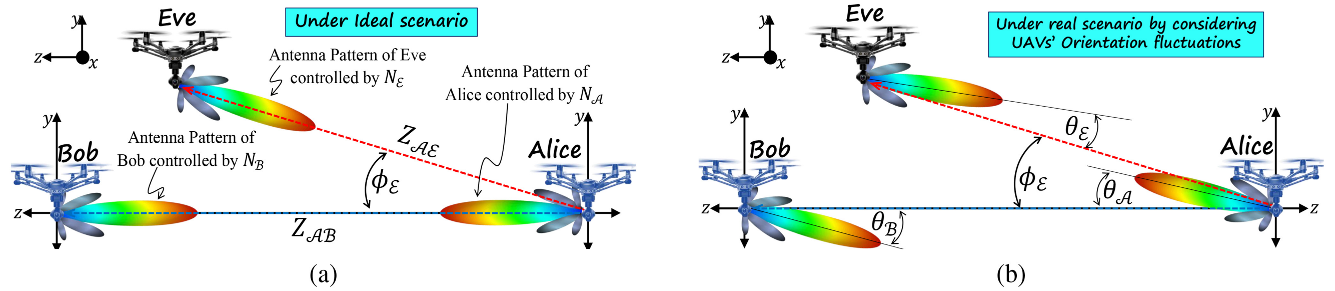

Eve
Under Ideal scenario
Antenna Pattern of Eve controlled by $N_{\mathcal{E}}$
Antenna Pattern of Alice controlled by $N_{\mathcal{A}}$
Antenna Pattern of Bob controlled by $N_{\mathcal{B}}$
Bob
Alice
$Z_{\mathcal{AE}}$
$\phi_{\mathcal{E}}$
$Z_{\mathcal{AB}}$
y
x
z
(a)
Eve
Under real scenario by considering UAVs' Orientation fluctuations
Bob
Alice
$\theta_{\mathcal{E}}$
$\phi_{\mathcal{E}}$
$\theta_{\mathcal{A}}$
$\theta_{\mathcal{B}}$
(b)

FIGURE 1. Graphical illustration of the considered system model (a) In the ideal scenario that $\mathcal{A}$ communicates with $\mathcal{B}$ using directional mmWave antennas so that $\mathcal{E}$ is hovering at distance $Z_{\mathcal{AE}}$ and angle $\phi_{\mathcal{E}}$. (b) In real conditions, the directional beams deviate from their main directions.

UAVs is Nakagami-m model [35]. As such, the pdf of the random variable $\omega = |h|^2$ follows Gamma distribution, denoted by $f_{|H|^2}(\omega)$ is expressed as follows

$$f_{|H|^2}(\omega) = \frac{m^m \omega^{m-1}}{\Gamma(m)} \exp(-m\omega), \quad \text{for} \quad \omega > 0, \tag{13}$$

where m is the Nakagmi parameter and $\Gamma(\cdot)$ is the well-known Gamma function.

A. EAVESDROPPER MODEL

The system model also includes a third entity represented by an eavesdropper, denoted by $\mathcal{E}$. Similar to $\mathcal{A}$ and $\mathcal{B}$, $\mathcal{E}$ is a UAV hovering in the surrounding area of $\mathcal{B}$. Being an eavesdropper, $\mathcal{E}$ tries to capture the signal emitted from $\mathcal{A}$ towards $\mathcal{B}$, decodes it and retrieves the data transmitted. It is assumed that $\mathcal{E}$ has the same resources as in $\mathcal{B}$ and encounters the same position and orientation fluctuations with different values. To this end, the same notations used to denote $\mathcal{B}$'s parameters are utilized for $\mathcal{E}$ by replacing the subscript $\mathcal{B}$ by $\mathcal{E}$.

As transmissions is performed over the mmWave band, both the distance between $\mathcal{A}$ and $\mathcal{E}$, denoted by $Z_{\mathcal{AE}}$, and the relative position of $\mathcal{E}$ with respect to $\mathcal{A}$ and $\mathcal{B}$ are of paramount importance to evaluate the reception at both $\mathcal{B}$ and $\mathcal{E}$. Specifically, three different scenarios can be illustrated. The first scenario occurs when $\mathcal{E}$ blocks the line-of-sight (LoS) of the $\mathcal{A} - \mathcal{B}$ link, while the second scenario occurs when $\mathcal{B}$ blocks the LoS of the $\mathcal{A} - \mathcal{E}$ link. The third scenario is represented when both the first and second scenarios do not occur, i.e., neither $\mathcal{E}$ blocks the LoS of the $\mathcal{A} - \mathcal{B}$ nor $\mathcal{B}$ blocks the LoS of the $\mathcal{A} - \mathcal{B}$ link. In our study, only the third scenario is considered while the other two scenarios are ignored. The reason behind this can be interpreted as follows. In the first scenario, $\mathcal{B}$ can easily realize that the LoS signal from $\mathcal{A}$ is blocked, which leads to ask $\mathcal{A}$ to terminate the data transmission to avoid potential eavesdropping. On the other hand, in the second scenario, the signal received at $\mathcal{E}$ is very low due to blocking the LoS, which makes the system inherently secure. However, the third scenario is worth to be investigated as $\mathcal{E}$ is able, based on its exact relative location, to capture a significant level of the transmitted signal, and therefore, poses a significant threat to the confidentiality of the transmitted data.

III. CAPACITY AND SECRECY ANALYSIS

In this section, three different metrics will be investigated for the considered UAV-based system, namely, the average channel capacity, the average secrecy capacity and the probability of strictly positive capacity.

A. AVERAGE CHANNEL CAPACITY

1) AVERAGE CHANNEL CAPACITY OF THE LINK $\mathcal{A} - \mathcal{B}$

The instantaneous channel capacity of the $\mathcal{A} - \mathcal{B}$ link, denoted by $C_{\mathcal{AB}}$, can be expressed as follows:

$$C_{\mathcal{AB}} = \log_2(1 + \gamma_1), \tag{14}$$

where γ_1 represents the received SNR at $\mathcal{B}$'s end. The average of $C_{\mathcal{AB}}$, denoted by $\overline{C}_{\mathcal{AB}}$, can be expressed as follows

$$\overline{C}_{\mathcal{AB}} = \int_0^\infty \log_2(1 + \gamma_1) f_{\gamma_1}(\gamma_1) d\gamma_1, \tag{15}$$

where the pdf $f_{\gamma_1}(\gamma_1)$ represents the probability density function (pdf) of γ_1. According to [10], $f_{\gamma_1}(\gamma_1)$ is given by

$$f_{\gamma_1}(\gamma_1) = \sum_{i=0}^{kD-1} \sum_{j=0}^{kD-1} \mathbb{R}_{i,j} \gamma_1^{m-1} \exp(-\mu_1 \gamma_1), \tag{16}$$

where D represents the number of antenna sectors considered, $k \in \{1, 2\}$ where $k = 1$ implies only the main lobe is considered, while $k = 2$ implies that the main and the first side lobes are considered. Moreover, $\mathbb{R}_{i,j}$ is formulated as

$$\begin{cases} \mathbb{R}_{i,j} = \frac{\mathbb{J}_{i,j}\left(\theta'_{\mathcal{A}xy}, \theta'_{\mathcal{B}xy}, \sigma^2_{\theta_\mathcal{A}}, \sigma^2_{\theta_\mathcal{B}}\right)}{\Gamma(m)} (\mu_1)^m, \\ \mathbb{J}_{i,j}\left(\theta'_{\mathcal{A}xy}, \theta'_{\mathcal{B}xy}, \sigma^2_{\theta_\mathcal{A}}, \sigma^2_{\theta_\mathcal{B}}\right) = J_i\left(\theta'_{\mathcal{A}xy}, \sigma^2_{\theta_\mathcal{A}}\right) J_j\left(\theta'_{\mathcal{B}xy}, \sigma^2_{\theta_\mathcal{B}}\right), \\ J_i\left(\theta'_{\mathcal{A}xy}, \sigma^2_{\theta_\mathcal{A}}\right) = M\left(\frac{\theta'_{\mathcal{A}xy}}{\sigma_{\theta_\mathcal{A}}}, \frac{i}{DN_\mathcal{A}\sigma_{\theta_\mathcal{A}}}\right) \\ \qquad\qquad - M\left(\frac{\theta'_{\mathcal{A}xy}}{\sigma_{\theta_\mathcal{A}}}, \frac{i+1}{DN_\mathcal{A}\sigma_{\theta_\mathcal{A}}}\right), \\ J_j\left(\theta'_{\mathcal{B}xy}, \sigma^2_{\theta_\mathcal{B}}\right) = M\left(\frac{\theta'_{\mathcal{B}xy}}{\sigma_{\theta_\mathcal{B}}}, \frac{j}{DN_\mathcal{B}\sigma_{\theta_\mathcal{B}}}\right) \\ \qquad\qquad - M\left(\frac{\theta'_{\mathcal{B}xy}}{\sigma_{\theta_\mathcal{B}}}, \frac{j+1}{DN_\mathcal{B}\sigma_{\theta_\mathcal{B}}}\right), \\ \mu_1 = \frac{m\sigma^2}{P_t h_{L_B} \mathbb{R}'_{i,j}}, \end{cases} \tag{17}$$

where

$$\mathbb{R}'_{i,j}\begin{cases}4\pi^4 G_0''^{(N_\mathcal{A})}G_0''^{(N_\mathcal{B})}, & \text{for } \ i=j=0,\\ 2\pi^2 G_0''^{(N_\mathcal{A})}G_0''^{(N_\mathcal{B})}\frac{D^2\left(1-\cos^2\left(\frac{i\pi}{D}\right)\right)}{i^2}, & \text{for } \ i\neq 0\ j=0,\\ 2\pi^2 G_0''^{(N_\mathcal{A})}G_0''^{(N_\mathcal{B})}\frac{D^2\left(1-\cos^2\left(\frac{j\pi}{D}\right)\right)}{j^2}, & \text{for } \ i=0\ j\neq 0,\\ 4G_0''^{(N_\mathcal{A})}G_0''^{(N_\mathcal{B})}\frac{D^4\sin^2\left(\frac{i\pi}{2D}\right)\sin^2\left(\frac{j\pi}{2D}\right)}{i^2j^2}, & \text{for } \ i\neq 0\ j\neq 0,\end{cases} \tag{18}$$

and

$$\begin{cases}G_0''^{(N_\mathcal{A})} = 0.2025\times 10^{\frac{G_{max}}{10}}G_0(N_\mathcal{A}),\\ G_0''^{(N_\mathcal{B})} = 0.2025\times 10^{\frac{G_{max}}{10}}G_0(N_\mathcal{B}).\end{cases} \tag{19}$$

Also, $\theta'_{\mathcal{Q}q_1q_2} = \sqrt{(\theta'_{\mathcal{Q}_{q_1}})^2 + (\theta'_{\mathcal{Q}_{q_2}})^2}$ where the subscripts $\mathcal{Q}$, q_1 and q_2 are $\mathcal{Q}\in\{\mathcal{A},\mathcal{B}\}$, $(q_1,q_2)\in\{x,y\}$.

Therefore, (15) can be rewritten by substituting $f_{\gamma_1}(\gamma_1)$ from (16) to yield

$$\overline{C}_{\mathcal{AB}} = \sum_{i=0}^{kD-1}\sum_{j=0}^{kD-1}\mathbb{R}_{i,j}\int_0^\infty \log_2(1+\gamma_1)\gamma_1^{m-1}\exp(-\mu_1\gamma_1)d\gamma_1, \tag{20}$$

Now, using [36, eq. (4.337.5)], the integral in (20) can be solved and expressed in terms of the exponential integral function Ei [36] as follows

$$\overline{C}_{\mathcal{AB}} = \sum_{i=0}^{kD-1}\sum_{j=0}^{kD-1}\frac{\mathbb{R}_{i,j}}{\mu_1^m\ln(2)}\sum_{u=0}^{m-1}\frac{(m-1)!}{(m-u-1)!} \times\left[\frac{(-1)^{m-u-2}}{\left(\frac{1}{\mu_1}\right)^{m-u-1}}e^{\mu_1}Ei(-\mu_1) + \sum_{s=1}^{m-u-1}(s-1)!(-\mu_1)^{m-u-s-1}\right], \tag{21}$$

2) AVERAGE CHANNEL CAPACITY OF THE LINK $\mathcal{A}-\mathcal{E}$:

The average channel capacity of the $\mathcal{A}-\mathcal{E}$ link, denoted by $\overline{C}_{\mathcal{AE}}$, can be computed by the exact the framework followed to obtain $\overline{C}_{\mathcal{AB}}$ expect using the pdf $f_{\gamma_2}(\gamma_2)$ where γ_2 represents the SNR of the $\mathcal{A}-\mathcal{E}$ link, given as follows [10]

$$f_{\gamma_2}(\gamma_2) = \sum_{p=0}^{kD-1}\sum_{q=J_{E1}D+1}^{J_{E2}D}\mathbb{K}_{p,q}\gamma_2^{m-1}\exp(-\mu_2\gamma_2), \tag{22}$$

where $J_{E1} = \max\{0, J_E - 1\}$, $J_{E2} = J_E + 2$, $J_E = \lfloor\phi_\mathcal{E}N_\mathcal{A}\rfloor$, and $\phi_\mathcal{E}$ is the spatial angle between Eve and the main link between Alice and Bob which is depicted in Fig. 1. In particular, $\phi_\mathcal{E}$ characterizes Eve's location relative to Alice and Bob. In this work, we show that $\phi_\mathcal{E}$ plays an important role in link security. Please note that the range $q\in\{J_{E1}D+1, J_{E2}D\}$ in (22) indicates the range of the sub-lobes of the Alice's antenna which is in the direction of Eve's antenna. Also, μ_2 is given as

TABLE 2. Parameter values used in the simulation.

Parameters	Values	Parameters	Values
$\phi_\mathcal{E}$	$0^o - 12^o$	m	2
$Z_{\mathcal{AE}}$	$300 - 500$ m	f_c	95.7 GHz
$Z_{\mathcal{AB}}$	500 m	$N_\mathcal{A}$	$2 - 60$
$\sigma_{\theta_\mathcal{E}}$	$0.5^o - 3^o$	$N_\mathcal{B}$	$2 - 40$
$\sigma_{\theta_\mathcal{A}}$	$0.5^o - 3^o$	$N_\mathcal{E}$	20
$\sigma_{\theta_\mathcal{B}}$	$0.5^o - 3^o$	P_t	7 dBm
$\theta'_{\mathcal{E}_x} = \theta'_{\mathcal{E}_y}$	0.1^o	σ^2	-89 dBm
$\theta'_{\mathcal{A}_x} = \theta'_{\mathcal{B}_x}$	0.1^o	$\theta'_{\mathcal{A}_y} = \theta'_{\mathcal{B}_y}$	0.15^o

$$\mu_2 = \frac{m\sigma^2}{P_th_{L_e}\mathbb{K}'_{p,q}}. \tag{23}$$

Notice that $\mathbb{K}_{p,q}$ and $\mathbb{K}'_{p,q}$ are computed as explained for $\mathbb{R}_{p,q}$ and $\mathbb{R}'_{p,q}$, respectively, taking into account replacing $\mathcal{B}$'s parameters by $\mathcal{E}$'s parameters.

$\overline{C}_{\mathcal{AE}}$ in its final expression is given as follows:

$$\overline{C}_{\mathcal{AE}} = \sum_{p=0}^{kD-1}\sum_{q=J_{E1}D+1}^{J_{E2}D}\frac{\mathbb{K}_{p,q}}{\mu_2^m\ln(2)}\sum_{u=0}^{m-1}\frac{(m-1)!}{(m-u-1)!} \times\left[\frac{(-1)^{m-u-2}}{\left(\frac{1}{\mu_2}\right)^{m-u-1}}e^{\mu_2}Ei(-\mu_2) + \sum_{s=1}^{m-u-1}(s-1)!(-\mu_2)^{m-u-s-1}\right]. \tag{24}$$

B. AVERAGE SECRECY CAPACITY

The instantaneous secrecy capacity C_S is defined as follows

$$\begin{aligned}C_s &= C_{\mathcal{AB}} - C_{\mathcal{AE}}\\ &= \log_2(1+\gamma_1) - \log_2(1+\gamma_2),\end{aligned} \tag{25}$$

As both γ_1 and γ_2 are independent random variables, the average secrecy capacity, $\overline{C}_s$, can be expressed as follows

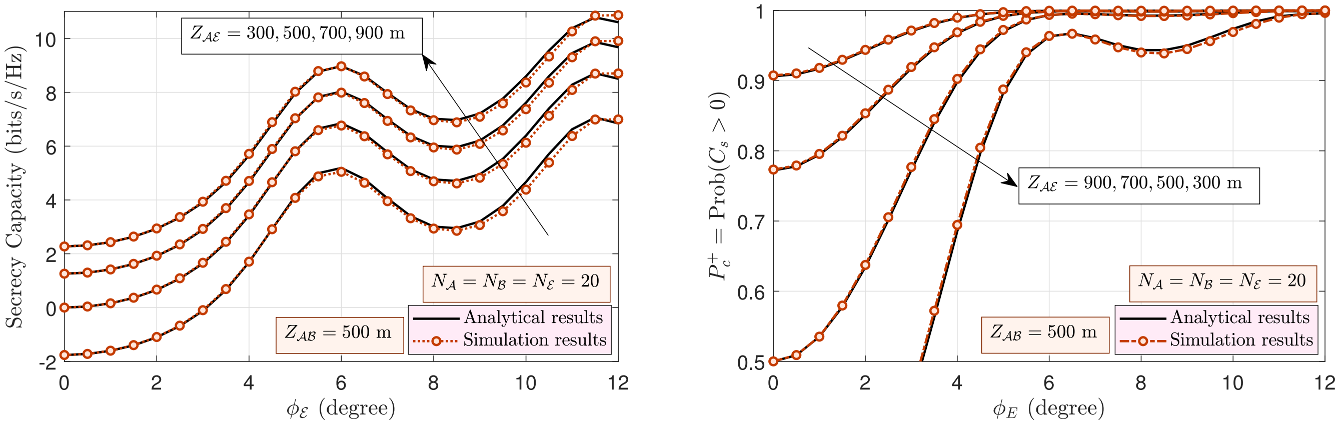
$$\overline{C}_s = \overline{C}_{\mathcal{AB}} - \overline{C}_{\mathcal{AE}}, \tag{26}$$

where both $\overline{C}_{\mathcal{AB}}$ and $\overline{C}_{\mathcal{AE}}$ have been derived in (21) and (24), respectively. As such, by substituting (21) and (24) into (26), the final formula of $\overline{C}_s$ can be obtained.

C. THE PROBABILITY OF STRICTLY POSITIVE CAPACITY

The probability of strictly positive secrecy capacity (SPSC) is usually defined as the probability that the secrecy capacity is larger than zero, and it is mathematically expressed as follows

$$\begin{aligned}P_s^+ &= \text{Prob.}(C_s > 0)\\ &= \text{Prob.}\big(\log_2(1+\gamma_1) - \log_2(1+\gamma_2) > 0\big)\\ &= \text{Prob.}(\gamma_1 - \gamma_2 > 0)\\ &= \text{Prob.}(\Delta > 0)\\ &= 1 - F_\Delta(0),\end{aligned} \tag{27}$$



(a)

(b)

FIGURE 2. Comparison of link secrecy performance of the considered UAV-based system versus $\phi_{\mathcal{E}}$ and for different values of Z_{AE} for (a) $\bar{C}_s$ and (b) P_s^+.

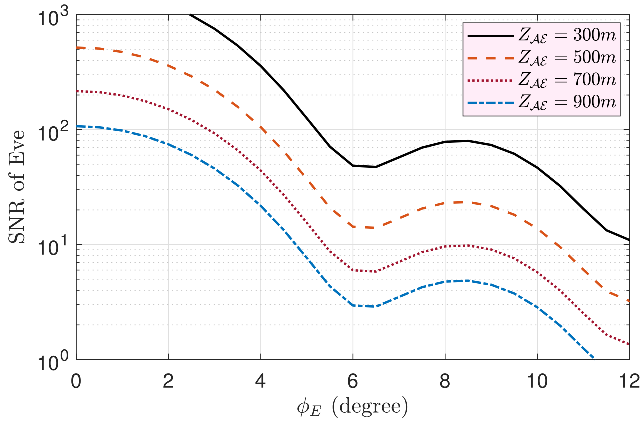


FIGURE 3. The effect of $Z_{\mathcal{AE}}$ and $\phi_{\mathcal{E}}$ parameters on Eve's SNR.

where $F_\Delta(\delta)$ is the CDF of the random variable $\Delta = \gamma_1 - \gamma_2$.

According to [37, eq. (6.55), page 186], the CDF of the random variable composed by the difference between two independent random variables, can be expressed as follows

$$F_\Delta(\delta) = \int_0^\infty \int_0^{\delta+\gamma_2} f_{\gamma_1}(\gamma_1) f_{\gamma_2}(\gamma_2) \cdot d\gamma_1 d\gamma_2, \quad \text{for} \quad \delta \geq 0 \tag{28}$$

which can be rewritten by substituting both pdfs to be

$$F_\Delta(\delta) = \sum_{i=0}^{kD-1} \sum_{j=0}^{kD-1} \sum_{p=0}^{kD-1} \sum_{q=J_{E1}D+1}^{J_{E2}D} \mathbb{K}_{p,q} \mathbb{R}_{i,j} \int_0^\infty \int_0^{\delta+\gamma_2} \gamma_1^{m-1} \exp(-\mu_1\gamma_1) \gamma_2^{m-1} \exp(-\mu_2\gamma_2) \cdot d\gamma_1 d\gamma_2. \tag{29}$$

Now, the inner integral of γ_1 in (29) can be solved using [36, eq. (2.321.2)]

$$F_\Delta(\delta) = \sum_{i=0}^{kD-1} \sum_{j=0}^{kD-1} \sum_{p=0}^{kD-1} \sum_{q=J_{E1}D+1}^{J_{E2}D} \mathbb{R}_{i,j} \mathbb{K}_{p,q} \int_0^\infty \left(-\sum_{t=0}^{m-1} \frac{t! \binom{m-1}{t} (\delta + \gamma_2)^{m-t-1}}{(\mu_1)^{t+1}} \exp(-\mu_1(\delta + \gamma_2)) + \frac{(m-1)!}{(\mu_1)^m} \right) \gamma_2^{m-1} \exp(-\mu_2\gamma_2)\, \mathrm{d}\gamma_2, \tag{30}$$

which can be expressed in terms of the integrals I_1 and I_2 to be

$$F_\Delta(\delta) = \sum_{i=0}^{kD-1} \sum_{j=0}^{kD-1} \sum_{p=0}^{kD-1} \sum_{q=J_{E1}D+1}^{J_{E2}D} \mathbb{R}_{i,j} \mathbb{K}_{p,q} \left(-\sum_{t=0}^{m-1} \frac{t! \binom{m-1}{t} \sum_{d=0}^{m-t-1} \binom{m-t-1}{d} \delta^{m-t-d-1} I_1}{(\mu_1)^{t+1}} + I_2 \right), \tag{31}$$

where the integrals I_1 and I_2 are given as

$$I_1 = \exp(-\mu_1\delta) \int_0^\infty \gamma_2^{d+m-1} \exp(-(\mu_1 + \mu_2)\gamma_2) d\gamma_2, \tag{32}$$

and

$$I_2 = \frac{(m-1)!}{(\mu_1)^m} \int_0^\infty \gamma_2^{m-1} \exp(-\mu_2\gamma_2) \cdot d\gamma_2, \tag{33}$$

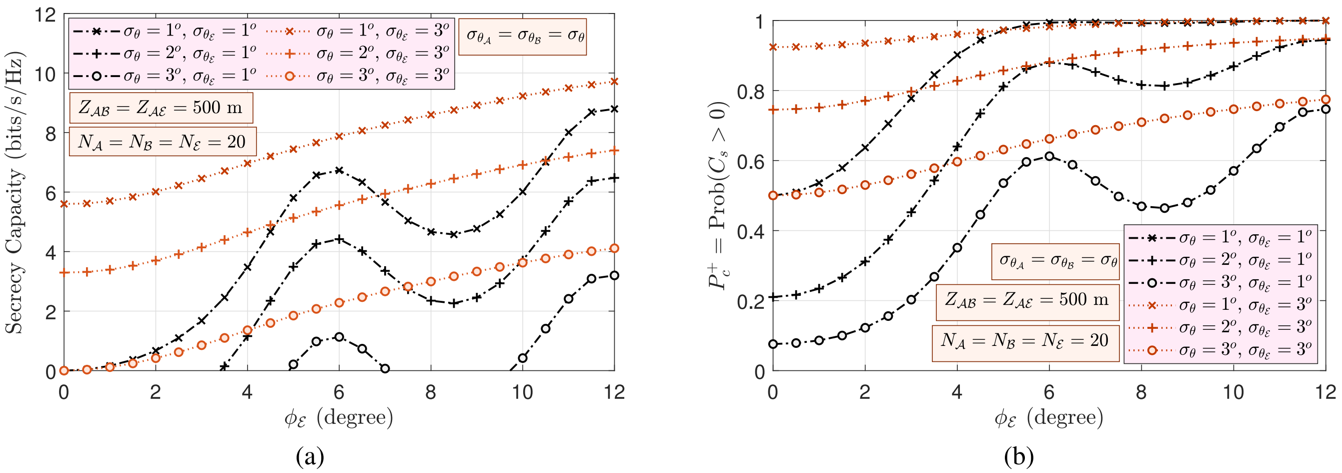
where both I_1 and I_2 can be solved also using [36, eq. (3.351.3)] to yield

$$I_1 = \exp(-\mu_1\delta)(d + m - 1)!(\mu_1 + \mu_2)^{-d-m}, \tag{34}$$

and

$$I_2 = \frac{((m-1)!)^2}{(\mu_1\mu_2)^m}. \tag{35}$$

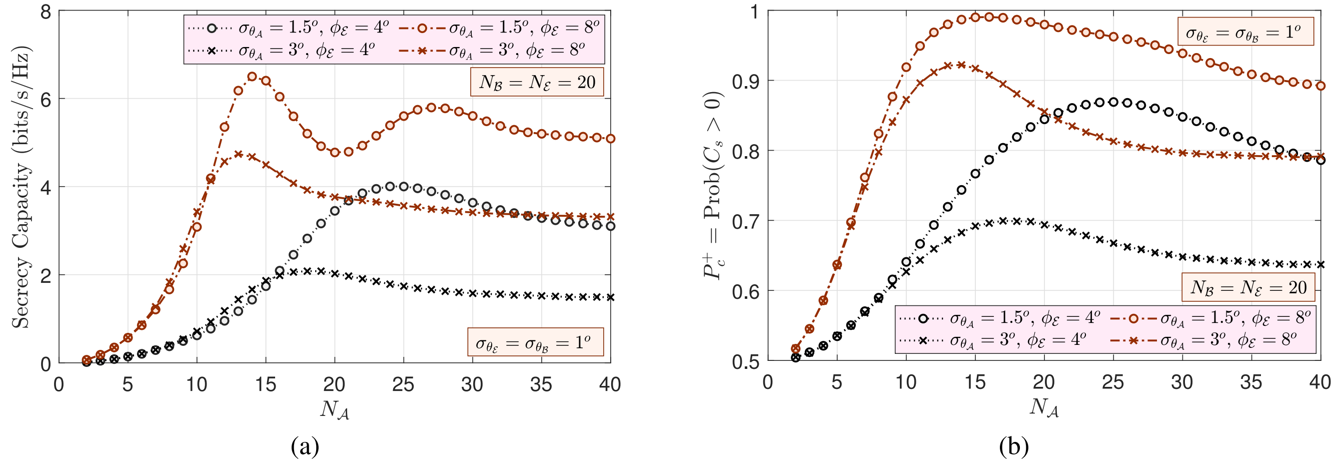
Therefore, $F_\Delta(\delta)$ can be obtained by substituting both I_1 and I_2 into (31). However, to get the PS^+, one needs first to compute $F_\Delta(0)$, which can be expressed as follows



(a)

(b)

FIGURE 4. Comparison of link secrecy performance of the considered UAV-based system versus $\phi_\mathcal{E}$ and for different values of σ_{θ_A} and σ_{θ_B} for (a) $\bar{C}_s$ and (b) P_s^+.



(a)

(b)

FIGURE 5. Comparison of link secrecy performance of the considered UAV-based system versus N_A and for different values of σ_{θ_A} and $\phi_\mathcal{E}$ for (a) $\bar{C}_s$, and (b) P_s^+.

$$F_\Delta(0) = \sum_{i=0}^{kD-1}\sum_{j=0}^{kD-1}\sum_{p=0}^{kD-1}\sum_{q=J_{E1}D+1}^{J_{E2}D} \mathbb{R}_{i,j}\mathbb{K}_{p,q} \left(\frac{((m-1)!)^2}{(\mu_1\mu_2)^m} - \sum_{t=0}^{m-1}\frac{t!\binom{m-1}{t}(2m-t-2)(\mu_1+\mu_2)^{-2m+t+1}}{(\mu_1)^{t+1}}\right), \quad (36)$$

which can be substituted into (27) to get the final closed form expression of SPSC as given in (37) in the bottom of this page.

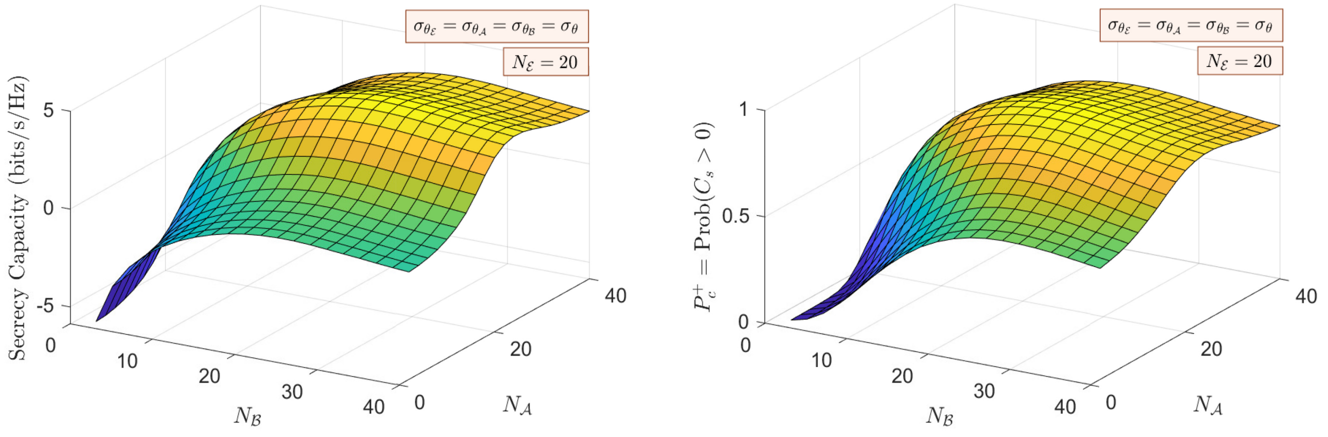
IV. RESULTS AND DISCUSSION

In this section, analytical and simulation results of the secrecy performance of the considered UAV-based link are examined. In the results, parameters are either fixed or variable over a specific range as listed in Table 2. These parameters include $\phi_\mathcal{E}$, and $Z_{\mathcal{AE}}$, which specify the spatial angle and location of the $\mathcal{E}$ relative to the main link, respectively, (please see Fig. 1), $\sigma_{\theta\mathcal{A}}$, $\sigma_{\theta\mathcal{B}}$, and $\sigma_{\theta\mathcal{E}}$ which determine the UAVs' orientation of $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{E}$, respectively, $N_\mathcal{A}$, $N_\mathcal{B}$, and $N_\mathcal{E}$ that characterize the array antenna patterns of $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{E}$, respectively.

For the Monte Carlo simulations, we first generated 10^7 independent random values of random variables $\theta_{\mathcal{A}x}$, $\theta_{\mathcal{A}y}$, $\theta_{\mathcal{B}x}$, $\theta_{\mathcal{B}y}$, $\theta_{\mathcal{E}x}$, and $\theta_{\mathcal{E}y}$. Then, using (1) and (2), we generated 10^7 random values of $\theta_\mathcal{A}$, $\Phi_\mathcal{A}$, $\theta_\mathcal{B}$, $\Phi_\mathcal{B}$, $\theta_\mathcal{E}$, and $\Phi_\mathcal{E}$. After that, using (3), (9) and (11), we generated 10^7 random values of γ_1 and γ_2. Finally, using the obtained random values for γ_1 and γ_2, we compute $\bar{C}_s$ and P_s^+.

It should be noted that, unlike the works in the literature that generally use approximate antenna patterns to obtain the closed-form expressions, in this work, we obtained the closed-form of $\bar{C}_s$ and P_s^+ based on actual

$$P_s^+ = 1 - \sum_{i=0}^{kD-1}\sum_{j=0}^{kD-1}\sum_{p=0}^{kD-1}\sum_{q=J_{E1}D+1}^{J_{E2}D} \mathbb{R}_{i,j}\mathbb{K}_{p,q} \left(\frac{((m-1)!)^2}{(\mu_1\mu_2)^m} - \sum_{t=0}^{m-1}\frac{t!\binom{m-1}{t}(2m-t-2)(\mu_1+\mu_2)^{-2m+t+1}}{(\mu_1)^{t+1}}\right). \quad (37)$$



(a) (b)

FIGURE 6. Comparison of link secrecy performance of the considered UAV-based system versus N_A and N_B for (a) $\bar{C}_s$, and (b) P_s^+.

antenna pattern. In Fig. 2, both the simulation and analytical results of $\bar{C}_s$ and P_s^+ are depicted versus the angle *phi*$_\mathcal{E}$ ($\phi_\mathcal{E} \in \{0^o, \ldots, 12^o\}$ and considering different values of the distance $Z_{\mathcal{AE}}$ ($Z_{\mathcal{AE}} =$ 300, 500, 700, and 900m). We also consider $Z_{\mathcal{AB}} = 500$m, $\sigma_{\theta_\mathcal{A}} = \sigma_{\theta_\mathcal{B}} = \sigma_{\theta_\mathcal{E}} = 1^o$, and $N_\mathcal{A} = N_\mathcal{B} = N_\mathcal{E} = 20$. The first observation which can be made is that analytical and simulation results exactly match each other, which verifies the accuracy of the obtained closed form expressions in this work. Another observation is that both $\bar{C}_s$ and P_s^+ improve as $\phi_\mathcal{E}$ increases, which is mainly due to increasing the deviation between the location of $\mathcal{E}$ and the main lobe between $\mathcal{A}$ and $\mathcal{B}$. Moreover, the impact of increasing the distance $Z_{\mathcal{AE}}$ is clearly shown as it improving both $\bar{C}_s$ and P_s^+ due the degradation of the received SNR at $\mathcal{E}$. To get a better view, in Fig. 3, the effect of parameters $\phi_\mathcal{E}$ on the SNR of Eve is investigated. As we can see, there is a direct relationship between Eve's SNR and metrics $\bar{C}_s$ and P_s^+. A final observation that can be obtained from Fig. 2 is that both $\bar{C}_s$ and P_s^+ show non-uniformity on their performance where they both pass through consecutive fluctuation as $\phi_\mathcal{E}$ increases. This can be referred to antenna radiation pattern of the antenna that includes several side-lobes leading to variable received SNR at $\mathcal{E}$ as $\phi_\mathcal{E}$ increases.

Another parameter affecting secrecy is the ratio of σ_{θ_A} (intensity of UAV's vibration of $\mathcal{A}$) to σ_{θ_E} (intensity of UAV's vibration of $\mathcal{E}$). It should be noted that since $\mathcal{A}$ is the transmitter, the severity of its angular fluctuations has a greater impact on the secrecy link compared to $\mathcal{B}$. Therefore, using simulations, in Fig. 4, both $\bar{C}_s$ and P_s^+ of the considered UAV-based system are plotted versus $\mathcal{E}$ for different values of $\sigma_{\theta_\mathcal{A}} = 1^o, 2^o$, and 3^o, as well as two different values $\sigma_{\theta_\mathcal{E}} = 1^o$ and 3^o. The distances are set to $Z_{\mathcal{AB}} = Z_{\mathcal{AE}} = 500$m and $N_\mathcal{A} = N_\mathcal{B} = N_\mathcal{E} = 20$. The results in Fig. 4 clearly show that in order to increase the link secrecy, it is necessary to reduce the intensity of the UAV's fluctuations of $\mathcal{A}$. Specifically, it can be seen that decreasing (increasing) the fluctuation intensities of $\mathcal{A}$ ($\mathcal{E}$) will positively impact the secrecy performance.

TABLE 3. Find optimal values for N_A and N_B for different values of σ_{θ_A} and $\phi_\mathcal{E}$.

		Strictly Pos. Cap.			Secrecy capacity		
$\phi_\mathcal{E}$	$\sigma_{\theta_\mathcal{A}}$	$N_\mathcal{A}$	$N_\mathcal{B}$	P_s^+	$N_\mathcal{A}$	$N_\mathcal{B}$	$\overline{C_s}$
2^o	0.5^o	57	31	0.993	54	36	8.19
	1.5^o	14	30	0.926	32	37	4.21
	3^o	4	30	0.916	16	37	3.1
5^o	0.5^o	47	23	0.9999	46	36	10.88
	1.5^o	20	27	0.986	21	36	7.51
	3^o	8	29	0.936	15	37	4.85
10^o	0.5^o	48	20	$\simeq 1$	47	36	12.86
	1.5^o	13	23	0.999	23	36	9.39
	3^o	10	27	0.986	11	38	7.49

The antenna patterns have also a key role of the secrecy performance of the considered UAV-based link, which are adjusted with $N_\mathcal{A}$, $N_\mathcal{B}$, and $N_\mathcal{E}$. In Fig. 5, by using simulations, the secrecy performance (in terms of $\bar{C}_s$ and P_s^+) of the considered system is plotted versus $N_\mathcal{A}$ for different values of $\sigma_{\theta_\mathcal{A}}$ and $\phi_\mathcal{E}$. It is clear that the increasing the value of $N_\mathcal{A}$ does not always enhance $\bar{C}_s$ (or P_s^+), where it can be noted that there is an optimal value of $N_\mathcal{A}$ that maximize both $\bar{C}_s$ and P_s^+. As shown, the optimal value of $N_\mathcal{A}$ changes by changing setup parameters, such as the location of $\mathcal{E}$ or the intensity of the UAV's fluctuations. For example, for $\sigma_{\theta_\mathcal{A}} = 1.5^o$ and $\phi_\mathcal{E} = 4^o$, in term of P_s^+, the optimal value for $N_\mathcal{A}$ is 25, while for $\phi_\mathcal{E} = 8^o$, the optimal value of $N_\mathcal{A}$ decreases to 14. In Fig. 6, we examine the simultaneous effect of the antenna patterns of $\mathcal{A}$ and $\mathcal{B}$ for both metrics P_s^+ and $\bar{C}_s$. The simulation results clearly show that the optimal selection of the antenna patterns of both $\mathcal{A}$ and $\mathcal{B}$ is very important to improve channel secrecy in the presence of UAV's fluctuations. Therefore, in Table 3, the optimal values for $N_\mathcal{A}$ and $N_\mathcal{B}$ that maximize P_s^+ and $\bar{C}_s$ for nine different combinations of $\phi_\mathcal{E} = \{2^o, 5^o, 10^o\}$ and $\sigma_{\theta_\mathcal{A}} = \{0.5^o, 1.5^o, 3^o\}$ are listed. A general observation is that the optimal value of $N_{\mathcal{A}}$ significantly changes as either $\phi_{\mathcal{E}}$ or $\sigma_{\theta_{\mathcal{A}}}$ changes. On the other hand, changing either $\phi_{\mathcal{E}}$ or $\sigma_{\theta_{\mathcal{A}}}$ slightly changes the optimal value of $N_{\mathcal{B}}$. This may refer to the fact that $\mathcal{A}$ acts as a transmitter, and thus, its antenna pattern significantly impacts the performance. Also, it is worthy noting that increasing either $\phi_{\mathcal{E}}$ or $\sigma_{\theta_{\mathcal{A}}}$ decreases the optimal value of $N_{\mathcal{A}}$. For example, the maximum P_s^+ is achieved with $N_{\mathcal{A}} = 57$ for ($\phi_{\mathcal{E}} = 2^o, \sigma_{\theta_{\mathcal{A}}} = 0.5^o$), while $N_{\mathcal{A}} = 4$ and $N_{\mathcal{A}} = 47$ only can attain the maximum P_s^+ for ($\phi_{\mathcal{E}} = 2^o, \sigma_{\theta_{\mathcal{A}}} = 3^o$) and ($\phi_{\mathcal{E}} = 5^o, \sigma_{\theta_{\mathcal{A}}} = 0.5^o$), respectively.

V. CONCLUSION

In this paper, we investigated the secrecy of the UAV-based systems that used directional millimeter wave antennas under real scenarios including channel conditions, UAVs' vibrations, 3D real antenna patterns, and high-frequency attenuation of the millimeter wave band. After a detailed mathematical modeling of the considered system, the closed-form expressions of the average channel capacity, the average secrecy capacity and the probability of strictly positive secrecy capacity are derived and validated. Moreover, using extensive Monte Carlo simulations, the effects of different involved parameters including the location and spatial angle of the eavesdropper, the antenna pattern, and the intensity of UAVs' vibrations on the secrecy performance are investigated. Analytical and simulation results showed that UAVs' fluctuations have a significant impact on the secrecy performance, where reducing the fluctuation at the legitimate UAVs will improve the secrecy performance. Also, results showed that the antennas' patterns should be optimized to maximize the secrecy capacity of the UAV-based systems.

ACKNOWLEDGMENT

Open Access funding provided by the Qatar National Library.

REFERENCES

[1] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 619–641, 2nd Quart., 2014.

[2] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications,"in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, New Orleans, LA, USA, Mar. 2015, pp. 329–334.

[3] 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.

[4] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.

[5] Y. Zeng, J. Lyu, and R. Zhang, "Cellular-connected UAV: Potential, challenges, and promising technologies," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 120–127, Feb. 2019.

[6] X. Lin et al., "The sky is not the limit: LTE for unmanned aerial vehicles," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 204–210, Apr. 2018.

[7] D. W. Matolak and R. Sun, "Air–ground channel characterization for unmanned aircraft systems—Part I: Methods, measurements, and models for over-water settings," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 26–44, Jan. 2017.

[8] Y. Zheng, Y. Wang, and F. Meng, "Modeling and simulation of pathloss and fading for air-ground link of HAPs within a network simulator," in *Proc. IEEE Int. Conf. Cyber Enabl. Distrib. Comput. Knowl. Disc. (CyberC)*, Beijing, China, Oct. 2013, pp. 421–426.

[9] I. Bor-Yaliniz and H. Yanikomeroglu, "The new frontier in RAN heterogeneity: Multi-tier drone-cells," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 48–55, Nov. 2016.

[10] M. T. Dabiri, M. Rezaee, V. Yazdanian, B. Maham, W. Saad, and C. S. Hong, "3D channel characterization and performance analysis of UAV-assisted millimeter wave links," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 110–125, Jan. 2021.

[11] M. T. Dabiri, M. Rezaee, I. S. Ansari, and V. Yazdanian, "Channel modeling for UAV-based optical wireless links with nonzero boresight pointing errors," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 14238–14246, Dec. 2020.

[12] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (UAVs) for energy-efficient Internet of Things communications," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7574–7589, Nov. 2017.

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

[14] V. V. Chetlur and H. S. Dhillon, "Downlink coverage analysis for a finite 3-D wireless network of unmanned aerial vehicles," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4543–4558, Oct. 2017.

[15] A. M. Hayajneh, S. A. R. Zaidi, D. C. McLernon, and M. Ghogho, "Optimal dimensioning and performance analysis of drone-based wireless communications,"in *Proc. IEEE GLOBECOM Workshops*, Dec. 2016, pp. 1–6.

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

[17] P. Zhan, K. Yu, and A. L. Swindlehurst, "Wireless relay communications with unmanned aerial vehicles: Performance and optimization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 3, pp. 2068–2085, Jul. 2011.

[18] W. Guo, C. Devine, and S. Wang, "Performance analysis of micro unmanned airborne communication relays for cellular networks," in *Proc. IEEE Int. Symp. Commun. Syst. Netw. Digit. Signal Process. (CSNDSP)*, Manchester, U.K., Jul. 2014, pp. 658–663.

[19] 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.

[20] C. O. Nnamani, M. R. A. Khandaker, and M. Sellathurai, "UAV-aided jamming for secure ground communication with unknown eavesdropper location," *IEEE Access*, vol. 8, pp. 72881–72892, 2020.

[21] H. Lei et al., "Safeguarding UAV IoT communication systems against randomly located eavesdroppers," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1230–1244, Feb. 2020.

[22] L. Wei, K. Wang, C. Pan, and M. Elkashlan, "Secrecy performance analysis of RIS-aided communication system with randomly flying eavesdroppers," *IEEE Wireless Commun. Letters*, vol. 11, no. 10, pp. 2240–2244, Oct. 2022.

[23] H. Long et al., "Joint trajectory and passive beamforming design for secure UAV networks with RIS," in *Proc. IEEE Globecom Workshops*, Taipei, Taiwan, 2020, pp. 1–6,

[24] X. Yuan, Z. Feng, W. Ni, Z. Wei, R. P. Liu, and J. A. Zhang, "Secrecy rate analysis against aerial eavesdropper," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7027–7042, Oct. 2019

[25] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via trajectory optimization," in *Proc. IEEE Global Commun. Conf.*, Singapore, 2017, pp. 1–6,

[26] 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 Trans. Veh. Technol.*, vol. 70, no. 1, pp. 572–584, Jan. 2021.

[27] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, "Secure UAV-to-UAV systems with spatially random UAVs," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 564–567, Apr. 2019.

[28] X. Sun, W. Yang, Y. Cai, and M. Wang, "Secure mmWave UAV-enabled SWIPT networks based on random frequency diverse arrays," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 528–540, Jan. 2021.

[29] L. Zhang et al., "A survey on 5G millimeter wave communications for UAV-assisted wireless networks," *IEEE Access*, vol. 7, pp. 117460–117504, 2019.

[30] M. T. Dabiri, S. M. S. Sadough, and M. A. Khalighi, "Channel modeling and parameter optimization for hovering UAV-based free-space optical links," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 2104–2113, Sep. 2018.

[31] A. Kaadan, H. H. Refai, and P. G. LoPresti, "Multielement FSO transceivers alignment for inter-UAV communications," *J. Lightw. Technol.*, vol. 32, no. 24, pp. 4785–4795, Dec. 15, 2014.

[32] *Technical Specification Group Radio Access Network; Study of Radio Frequency (RF) and Electromagnetic Compatibility (EMC) Requirements for Active Antenna Array System (AAS) Base Station, Standard V*, 3GPP Standard TR 37.840, 2013.

[33] C. A. Balanis, *Antenna Theory: Analysis and Design*. Hoboken, NJ, USA: Wiley, 2016.

[34] *Study on Channel Model for Frequencies From 0.5 to 100 GHz (Release 14), V14.1.1*, 3GPP Standard TR 38.901, Jul. 2017.

[35] N. Goddemeier and C. Wietfeld, "Investigation of air-to-air channel characteristics and a UAV specific extension to the rice model," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2015, pp. 1–5.

[36] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2014.

[37] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. New York, NY, USA: McGraw Hill, 2002.