Received 17 December 2022; accepted 18 December 2022. Date of publication 2 January 2023;
date of current version 23 January 2023. The review of this article was coordinated by Editor Lina Mohjazi.

Digital Object Identifier 10.1109/OJVT.2022.3232272

Optical HAPS Eavesdropping in Vertical Heterogeneous Networks

EYLEM ERDOGAN [1] (Senior Member, IEEE), OLFA BEN YAHIA [2] (Member, IEEE),
GUNES KARABULUT KURT [2] (Senior Member, IEEE), AND HALIM YANIKOMEROGLU [3] (Fellow, IEEE)

[1] Department of Electrical and Electronics Engineering, Istanbul Medeniyet University, 34720 Istanbul, Turkey
[2] Department of Electrical Engineering, Polytechnique Montréal, Montréal, QC H3T 1J4, Canada
[3] Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada

CORRESPONDING AUTHOR: EYLEM ERDOGAN (e-mail: erdoganeyl@gmail.com)

ABSTRACT In the next generation (6G) wireless networks, the integration of terrestrial and non-terrestrial networks is essential to provide flawless connectivity over the globe. The vital element of this architecture is the high altitude platform station (HAPS) systems, which can provide reliable and ubiquitous connectivity among satellites, unmanned aerial vehicles (UAVs), and terrestrial users. Motivated by the importance of HAPS systems, in this paper, we provide three different use-cases for HAPS eavesdropping scenarios and investigate their physical layer security (PLS) performances. To quantify the PLS performance of the proposed setups, we perform secrecy outage probability (SOP), probability of positive secrecy (PPSC), average secrecy capacity (ASC), and secrecy throughput (ST) analyses. Furthermore, we also provide important design guidelines that can be beneficial for secure HAPS systems.

INDEX TERMS HAPS systems, optical communication, satellites, UAVs, PLS.

I. INTRODUCTION

The need for ubiquitous, flawless distance-insensitive wireless connectivity that can provide wide service coverage and high-fidelity services for all users, can be achieved by the unique integration of terrestrial and non-terrestrial networks (NTNs) for next-generation communication systems. This vision is also consistent with the Third Generation Partnership Project (3GPP) activities as defined in TR 38.811 [1]. The integration of terrestrial and NTNs is also envisioned by the Vertical heterogeneous network (VHetNet) architecture, which is a three-layer Vertical communication model consisting of a satellites network, aerial network and terrestrial network within the context of Sixth Generation (6G) vision [2]. In this architecture, the aerial network is composed of two sub-layers depending on the altitude and functionalities. The first sub-layer is comprised of high altitude platform station (HAPS) systems, whereas the second sub-layer is composed of unmanned aerial vehicle (UAV) nodes [3], [4].

An integral part of this architecture that has the ability to work as a backbone network to provide flawless connectivity among the elements of VHetNet architecture is the HAPS system. A HAPS can be defined as a flying vehicle operating in the stratosphere at an altitude between 18 to 50 km [5]. A HAPS node can be designed as a helium-filled airship and stay at a specified, nominal, fixed point relative to the Earth, above the atmospheric effects, civil air routes, and jet streams. Due to its unique characteristics, a HAPS can stay at a quasi-stationary position and provide ultra-wide coverage and high capacity [6].

To provide seamless connectivity in the VHetNet architecture, free space optical (FSO) communication can be an important enabler as it relies on license-free line-of-sight (LOS) point-to-point narrow beams [7]. FSO communication can be described as the transmission of optical information through optical carriers over long distances by using light-emitting diodes or laser beams operating in the near-infrared (IR) band. Compared to its radio-frequency (RF) counterpart, it can bring significant advantages to the VHetNet architecture including Gigabit data rates, enhanced security, ease of implementation, energy efficiency, lower delay, and low cost. Despite its numerous advantages, FSO communication can be deteriorated by turbulence-induced fading which can be caused by the random fluctuations in the amplitude and phase of the optical beam depending on the wind speed and temperature variations. Furthermore, adverse weather conditions in the troposphere layer, radiation-based absorption, cosmic dust, ice crystals due to polar stratospheric clouds, sulfuric acid ingredients, and volcanic ash due to volcanic activity, can cause attenuation in the laser beam [8]. Likewise, beam wander, Doppler spread due to relative motion, and misalignment errors can be counted as the other important drawbacks for optical systems.

In the VHetNet architecture, the integration of terrestrial and NTNs are of utmost importance. In this context, a HAPS system, that is employed with FSO transceivers and positioned between the satellites and ground users, can be considered as a floating terminal providing flawless and ubiquitous inter-connectivity among the VHetNet architecture from the stratosphere [9]. In VHetNet architecture, secure information transfer is a critical problem that needs to be addressed in the 6*G* vision as almost all the internet access will be established above the ground. Contrary to the well-known fiber optical communication architecture which can provide maximum security performance through fiber cables, non-terrestrial vehicles are prone to interception. Specifically, in the UAV to ground communications, eavesdroppers can intercept the communication by positioning very close to the ground terminal, whereas a lightweight HAPS eavesdropper can capture the optical communication over HAPS systems. In UAV to ground communications, weather effects can decrease the overall secrecy performance of the system and pointing losses may occur, whereas transmission distance can be a crucial problem in HAPS communications, which limits the security performance.

So far, communication security has been provided by using cryptography methods. Recently, an alternative technology, physical layer security (PLS) has been proposed to address the security problem of wireless systems in the physical layer by using the randomness of the wireless channels [10]. PLS is the most recent and easy to use security performance concept that can be used in NTNs [11], [12]. To this end, PLS has attracted several interests from academia and industry. PLS can be provided as long as the capacity of the main channel is superior to the capacity of the eavesdropper channel. In this context, three secrecy performance metrics; secrecy outage probability (SOP), probability of positive secrecy capacity (PPSC), and average secrecy capacity (ASC) have been proposed based on Wyner's model. In the literature, there are a few works that consider the PLS of NTNs. Among them, references [13], [14], [15], [16], [17] consider the PLS of UAV systems, whereas only [18] considers the PLS performance of the optical low Earth orbit (LEO) satellites. Only in [13], the authors investigated the optical eavesdropping in NTNs by considering downlink HAPS and UAV eavesdropping scenarios, where SOP and PPSC expressions were obtained. Different from the above-mentioned studies, in this work, we consider the security of optical HAPS systems and discuss the PLS performance of three practical use-cases. Specifically, the paper makes the following contributions:

- We propose three use-cases for HAPS eavesdropping by considering ground-to-HAPS, HAPS-to-HAPS, and HAPS-to-LEO satellite communications. In all these scenarios, we assume that a lightweight HAPS eavesdropper is trying to intercept the optical communication.
- To quantify the performance of the proposed use-cases, we derive SOP, PPSC, ASC, and secrecy throughput (ST) for all use-cases.
- We also provide important design guidelines to enhance the security of optical HAPS systems.

The rest of this paper is organized as follows. In Section II, the atmospheric limiting factors are presented. The proposed system models are provided in Section III followed by the secrecy performance analysis in Section IV. In Section V, the numerical results are provided and analyzed. Finally, the conclusion is drawn in Section VI.

TABLE 1 Stratospheric Attenuation coefficient for different stratospheric aerosol models at $\lambda = 1550$ nm for $H = 19$ km

Stratospheric aerosol model	Attenuation coefficient (km^{-1})
Extreme volcanic	$\Psi \approx 2 \times 10^{-1}$
High volcanic	$\Psi \approx 5 \times 10^{-2}$
Moderate volcanic	$\Psi \approx 8 \times 10^{-3}$
Background	$\Psi \approx 10^{-4}$

II. ATMOSPHERE BASED LIMITING FACTORS

In this section, we provide the atmospheric limiting factors for the proposed use-cases.

A. STRATOSPHERE BASED ATTENUATION

In the stratosphere, communication is affected by adverse stratospheric conditions. Mainly, the stratosphere layer is free from clouds and adverse weather conditions including fog, snow, and rain. However, the aerosol condition should be taken into consideration in the stratosphere, especially in the HAPS-to-HAPS communication. Aerosols are dominated by volcanic eruptions which bring a significant amount of volcanic ash to the stratosphere leading to extreme aerosol absorption [8]. Table 1 shows extinction coefficients for different levels of volcanic activity. As seen, in extreme volcanic activity, the extinction coefficient can be as high as 0.1 km^{-1} when the HAPS is positioned at 19 km. In addition, polar stratospheric clouds, hurricanes, when the clouds move up into the stratosphere, and radiation-based absorption can affect HAPS-to-HAPS communications. By taking these adverse effects, we model the overall attenuation as

$$I_a^{\mathrm{S}} = \exp\left(-\rho^{\mathrm{H}} L^{\mathrm{H}}\right), \tag{1}$$

where ρ^{H} shows the extinction coefficient and L^{H} stands for the distance between two HAPS nodes.

B. TROPOSPHERE BASED ATTENUATION

In ground-to-uplink communication, the quality of the optical signal is subject to different atmospheric effects, weather conditions, turbulence, and random fluctuations during its

TABLE 2 Geometrical scattering parameters for various types of cloud and Fog at λ = 1550nm

Cloud		
Cloud type	**V(km)**	**Attenuation coefficient (dB/km)**
Cumulus	0.0280	6.0646×10^5
Altostratus	0.0369	4.6019×10^5
Nimbostratus	0.0429	3.9583×10^5
Stratus	0.0626	2.7126×10^5
Stratocumulus	0.0959	1.7707×10^5
Cirrus	64.66	0.0026×10^5
Thin cirrus	290.69	0.0006×10^5
Fog		
Dense	0.05	339.62
Thick	0.20	84.90
Moderate	0.50	33.96
Light	0.77	16.67
Thin	1.90	4.59

propagation through the atmosphere. The major factor is the atmospheric conditions including cloud formations, fog, dust, rain, and snow, yielding to scattering, absorption, and attenuation of the signal due to the variations in the refractive index of the transmission path as shown in Table 2. Among them, scattering can be defined as the redirection of energy by the particles existing in the transmission path. Scattering is generally effective in the troposphere for systems that are operating between 20 THz to 375 THz. Scattering can be divided into two groups, Mie scattering, and Rayleigh scattering.

1) MIE SCATTERING

Mie scattering can occur when the optical beam is affected by the particles with a diameter approximately equal to signal bandwidth. Mie scattering is not related to the signal wavelength and it is the primary source of losses for the NTNs that are operating between 150 to 375 THz frequencies. Mathematically, it can be expressed as [19]

$$\rho' = ah_E^3 + bh_E^2 + ch_E + d, \tag{2}$$

where ρ' denotes the extinction ratio, h_E stands for the height of the GS above the mean sea level (km), and a, b, c and d are the wavelength λ (μm)-dependent empirical coefficients, which can be expressed as

$$\begin{aligned} a &= -0.000545\lambda^2 + 0.002\lambda - 0.0038 \\ b &= 0.00628\lambda^2 - 0.0232\lambda + 0.0439 \\ c &= -0.028\lambda^2 + 0.101\lambda - 0.18 \\ d &= -0.228\lambda^3 + 0.922\lambda^2 - 1.26\lambda + 0.719, \end{aligned} \tag{3}$$

and the atmospheric attenuation due to Mie scattering (I_m) can be expressed

$$I_m = \exp\left(-\frac{\rho'}{\sin(\theta)}\right), \tag{4}$$

where θ is the elevation angle.

2) ATMOSPHERIC ATTENUATION

Atmospheric attenuation depends on the weather conditions and it can be modeled with Beer-Lambert law as

$$I_a^{\mathrm{U}} = \exp\left(-\rho^{\mathrm{U}} L^{\mathrm{U}}\right), \tag{5}$$

where I_a^{A} is the atmospheric attenuation, ρ^{A} is the extinction coefficient related with the troposphere and L^{A} is the distance between HAPS and ground station.

3) OTHER EFFECTS

- Rayleigh scattering is largely caused by the particles which are much smaller than the signal wavelength. Rayleigh scattering can create extra background noise for the receivers. However, it can be negligible for the systems that are operating below 375 THz.
- Pointing can be described as directing the outgoing beam to the receiver based on a prior transmitter and receiver location information. In optical communication, precise pointing is a vital issue as pointing errors cause huge performance loss due to mechanical misalignment, vibrations, relative velocity, or problems in tracking systems[1].

C. TURBULENCE INDUCED FADING

Turbulent motion of the atmosphere with the presence of temperature and pressure gradients causes fluctuations in the irradiance of the wave. These index-of-refraction fluctuations cause scintillation which leads to both the temporal variation in received power and the spatial variation within a receiver aperture. In optical communications, the magnitude of the turbulence is measured in terms of the refractive index structure parameter, and the quantitative measure of scintillation is the scintillation index (σ_I^2). The scintillation index shows the level of fluctuations. In the scintillation index, $\sigma_I^2 < 1$ shows weak fluctuations, whereas $\sigma_I^2 > 1$ refers to moderate and strong fluctuations. In the envisioned HAPS systems, scintillation is obtained as $\sigma_I^2 << 1$ for the HAPS-to-HAPS and HAPS-to-satellite communications.

Various statistical models have been proposed in the literature to model the turbulence-induced fading including Log-normal, K, Gamma-Gamma, and Exponentiated Weibull (EW). Among them, Log-normal fading is appropriate for weak fluctuations, K can precisely model the strong fluctuations, Gamma-Gamma and EW are more appropriate for a variety of turbulence conditions, where EW is more appropriate for larger diameter optical receivers [20].

III. COMMUNICATION SYSTEM MODELS

In this section, we first present three new use-cases for HAPS systems as illustrated in Fig. 1. Thereafter, we describe the statistical models.

[1] Herein, we neglect the pointing losses as tracking enabled optical beam is used in the uplink satellite communications.

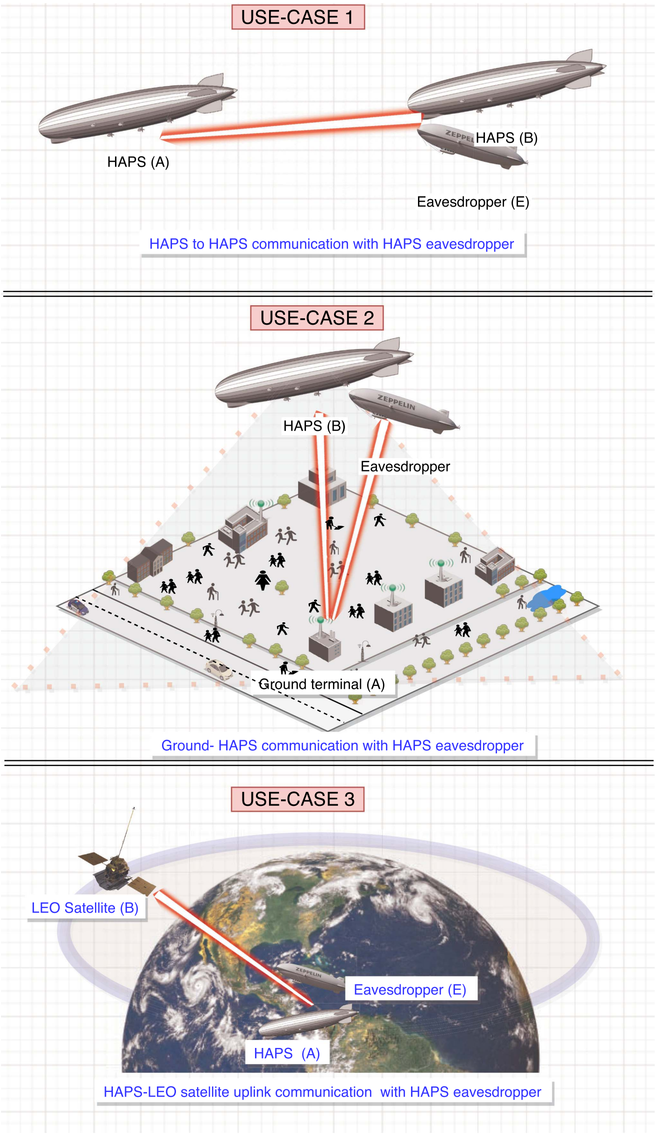
USE-CASE 1
HAPS (A)
HAPS (B)
Eavesdropper (E)
HAPS to HAPS communication with HAPS eavesdropper
USE-CASE 2
HAPS (B)
Eavesdropper
Ground terminal (A)
Ground- HAPS communication with HAPS eavesdropper
USE-CASE 3
LEO Satellite (B)
Eavesdropper (E)
HAPS (A)
HAPS-LEO satellite uplink communication with HAPS eavesdropper

FIGURE 1. **Illustration of HAPS eavesdropping use-cases.**

A. SYSTEM MODELS

1) USE-CASE 1: INTER-HAPS COMMUNICATION

In this scenario, we assume that a HAPS node A is communicating with a HAPS node B, and both of them are hovering at the same altitudes. In this use-case, we assume that an illegitimate ultralight stratospheric unmanned eavesdropper aircraft E located very close to B is trying to capture the information from A. In this scenario, E can be an illegitimate user or a legitimate user who has the intention of gathering the information of A. However, E can capture a small fraction of r_e of the refracted beam based stratospheric affects and wind. Furthermore, we assume that all nodes are affected by stratosphere-based attenuation.

2) USE-CASE 2: GROUND-HAPS UPLINK COMMUNICATION

In this use-case, we focus on the ground-to-HAPS communications where a ground station (GS) A is transmitting information to a HAPS node B in the presence of an ultralight stratospheric eavesdropper aircraft E. The ground station is close to mean sea level and affected adversely by weather conditions, and Mie scattering. These adverse effects scatter the beam and enable E to capture r_e fraction of the reflected beam.

3) USE-CASE 3: HAPS - LEO SATELLITE UPLINK COMMUNICATION

In the final use-case, we assume that a HAPS node A is communicating with an LEO satellite B in the presence of an ultralight stratospheric eavesdropper aircraft E which is located very close to A. In this scenario, we assume that the LEO satellite is deployed at about 500 km, whereas both A and E are located at about 19 km. We assume that turbulence-induced fading free communication model between A and E as E is positioned very close to A. Please note that the pointing loss due to the satellite's speed is neglected in this setup for a fair comparison of three use-cases. Moreover, all nodes are affected by light background radiation.

For all scenarios, the received signals at the nodes B and E can be expressed as

$$y_B = \sqrt{r_b P_A} h_B g_B + n_B, \tag{6}$$

and

$$y_E = \sqrt{r_e P_A} h_E g_E + n_E, \tag{7}$$

where P_A is the power of A, h_j is the attenuation depending on the use-case, and g_j is turbulence-induced fading, where $j \in \{B, E\}$. Noise samples n_B and n_E are given as additive white Gaussian with one-sided noise power spectral density N_0. By using (6) and (7), the SNRs can be written as

$$\gamma_B = r_b P_A \frac{h_B^2 |g_B|^2}{N_0}, \tag{8}$$

and

$$\gamma_E = r_e P_A \frac{h_E^2 |g_E|^2}{N_0}. \tag{9}$$

B. STATISTICAL MODELS

In all use-cases, we assume that the turbulence-induced fading follows EW distribution as it is the best fit for various aperture diameters in all fading levels. The probability density function (PDF) and the cumulative distribution function (CDF) of the EW fading channel can be expressed as [20]

$$f_{g_j}(I) = \frac{\alpha_j \beta_j}{\eta_j} \left(\frac{I}{\eta_j} \right)^{\beta_j - 1} \exp\left[- \left(\frac{I}{\eta_j} \right)^{\beta_j} \right] \times \left(1 - \exp\left[- \left(\frac{I}{\eta_j} \right)^{\beta_j} \right] \right)^{\alpha_j - 1} \tag{10}$$

and

$$\mathcal{F}_{g_j}(I) = \left(1 - \exp\left[- \left(\frac{I}{\eta_j} \right)^{\beta_j} \right] \right)^{\alpha_j}, \tag{11}$$

where α_j, β_j are the shape parameters and η_j is the scale parameter for $j \in \{B, E\}$. The fading parameters α_j, β_j, and

η_j can be expressed as [20]

$$\alpha_j = \frac{7.220 \times \sigma_{I_j}^{2/3}}{\Gamma\left(2.487\sigma_I^{2/6} - 0.104\right)},$$

$$\beta_j = 1.012\left(\alpha\sigma_I^2\right)^{-13/25} + 0.142$$

$$\eta_j = \frac{1}{\alpha\Gamma\left(1 + 1/\beta_j\right) g_1(\alpha_j, \beta_j)}, \tag{12}$$

where $g_1(\alpha_j, \beta_j)$ is the α_j and β_j dependent constant variable, which can be written as [20]

$$g_1(\alpha_j, \beta_j) = \sum_{k=0}^{\infty} \frac{(-1)^k \Gamma(\alpha_j)}{k!(k+1)^{1+1/\beta_j}\Gamma(\alpha_j - k)}, \tag{13}$$

and σ_I^2 denotes the scintillation index.

For the first use-case, we assume that A, B, and E are located at the same altitude. Thereby, the scintillation index for vertical communication can be written as

$$\sigma_{I_1}^2 = 1.23 C_n^2 \kappa^{7/6} L_{\mathrm{H}}^{11/7}, \tag{14}$$

where $\kappa = 2\pi/\lambda$ is the optical wave number, and $C_n^2(h)$ is the refractive index constant [19]

$$C_n^2(h) = 8.148 \times 10^{-56} \upsilon_r^2 h^{10} e^{-h/1000} + 2.7 \times 10^{-16} e^{-h/1500}$$
$$+ C_0 e^{-h/100} \quad m^{-2/3}, \tag{15}$$

where υ_r is the wind speed, and C_0 is the nominal value of the refractive index constant.

In the second use-case, we consider a ground-to-HAPS uplink optical communication with a tracked beam. Thereby, the scintillation index can be written as

$$\sigma_{I_2}^2 = \exp\left[\frac{0.49\sigma_R^2}{\left(1 + 1.11\sigma_R^{12/5}\right)^{7/6}} + \frac{0.51\sigma_R^2}{\left(1 + 0.69\sigma_R^{12/5}\right)^{5/6}}\right] - 1, \tag{16}$$

and the Rytov variance σ_R^2 can be expressed as [21, Section (12)]

$$\sigma_R^2 = 2.25\kappa^{7/6} \sec^{11/6}(\zeta) \int_{h_0}^{H} C_n^2(h)(h - h_0)^{5/6} dh, \tag{17}$$

where ζ is the zenith angle, h_0 stands for the height of the GS above ground level, and H is the altitude B and E.[21, Section (12)]

In the third use-case, E is located very close to B so that turbulence-induced fading can be negligible between B and E. However, the above-given PDF, CDF, and fading parameters can be used for A to B communication. The scintillation index for HAPS-to-satellite uplink communication can be expressed as

$$\sigma_{I_3}^2 = 2.2\varrho^{\frac{7}{6}} (h_{\mathrm{SAT}} - h_{\mathrm{HAPS}})^{5/6} \sec^{11/6}(\zeta)$$
$$\times \Re\left\{ \int_{h_0}^{H} C_n^2(\varpi)\left(1 - \frac{\varpi - h_{\mathrm{HAPS}}}{h_{\mathrm{SAT}} - h_{\mathrm{HAPS}}}\right)^{\frac{5}{6}} \right.$$
$$\left. \times \left(\frac{\varpi - h_{\mathrm{HAPS}}}{h_{\mathrm{SAT}} - h_{\mathrm{HAPS}}}\right)^{\frac{5}{6}} d\varpi \right\}. \tag{18}$$

where $\Re$ denotes the real-valued terms [21, Section (12)].

IV. SECRECY ANALYSIS

A. SECRECY OUTAGE PROBABILITY

In physical layer security, SOP is one of the most widely used secrecy criteria in the literature. In wireless communications, A has to transmit the information with a constant secrecy rate R_s providing that the secrecy capacity C_s is $C_s > R_s$. In that case, SOP can be defined as [22]

$$\begin{aligned} P_{\mathrm{SO}} &= \Pr[C_s < R_s], \\ &= \int_0^{\infty} F_{\gamma_B}(\gamma\gamma_{th} + \gamma_{th} - 1) f_{\gamma_E}(\gamma) d\gamma, \\ &\approx \int_0^{\infty} F_{\gamma_B}(\gamma\gamma_{th}) f_{\gamma_E}(\gamma) d\gamma, \end{aligned} \tag{19}$$

where $\gamma_{th} = 2^{R_s}$, and C_s can be written as

$$C_s = \begin{cases} \log_2(1 + \gamma_B) - \log_2(1 + \gamma_E), & \gamma_B > \gamma_E \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

1) USE-CASE 1 AND USE-CASE 2

To obtain the SOP expression for the first two use-cases, we first express the CDF of γ_B in a more tractable form by using Newton's Binomial theorem as [23]

$$F_{\gamma_B}(\gamma) = \sum_{\rho=0}^{\infty} \binom{\alpha_B}{\rho} (-1)^{\rho} \exp\left[-\rho\left(\frac{\gamma_B}{\eta_B^2 \overline{\gamma}_B}\right)^{\frac{\beta_B}{2}}\right], \tag{21}$$

and the PDF of γ_E can be written as

$$f_{\gamma_E}(\gamma) = \frac{\alpha_E \beta_E \gamma^{\frac{\beta_E}{2} - 1}}{2(\eta_E^2 \bar{\gamma}_E)^{\frac{\beta_E}{2}}} \left(1 - \exp\left[-\left(\frac{\gamma}{\eta_E^2 \bar{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right]\right)^{\alpha_E - 1}$$
$$\times \exp\left[-\left(\frac{\gamma}{\eta_E^2 \bar{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right]. \tag{22}$$

By using Newton's Binomial theorem, the above expression can be written in a more tractable form as [13]

$$f_{\gamma_E}(\gamma) = \frac{\alpha_E \beta_E \gamma^{\frac{\beta_E}{2} - 1}}{2(\eta_E^2 \bar{\gamma}_E)^{\frac{\beta_E}{2}}} \sum_{t=0}^{\infty} \binom{\alpha_E - 1}{t} (-1)^t$$
$$\times \exp\left[-(t+1)\left(\frac{\gamma}{\eta_E^2 \bar{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right]. \tag{23}$$

To obtain a closed-form SOP expression, we first assume that $\alpha_B = \alpha_E = \alpha$, $\beta_B = \beta_E = \beta$ and $\eta_B = \eta_E = \eta$. Thereafter, by invoking (23) and (21) into (19), with the aid of [24, eqn. (3.478.1)] and after a few theoretical manipulations, SOP can be written as

$$P_{\mathrm{SO}} = \frac{\alpha}{(\eta^2 \overline{\gamma}_E)^{\frac{\beta}{2}}} \sum_{\rho=0}^{\infty} \sum_{k=0}^{\infty} \binom{\alpha}{\rho} \binom{\alpha - 1}{k} (-1)^{\rho + k}$$
$$\times \left((k+1)\left(\frac{1}{\eta^2 \overline{\gamma}_E}\right) + \rho\left(\frac{\gamma_{th}}{\eta^2 \overline{\gamma}_B}\right)\right)^{-\frac{\beta}{2}}. \tag{24}$$

From (24), we can realize that when $\bar{\gamma}_E \to 0$, $P_{\mathrm{SO}} \to 0$. This shows us that perfect secrecy can be established when $\bar{\gamma}_E \to 0$.

2) USE-CASE 3

In the third scenario, we assume a turbulence-free communication model between B and E as they are located close to each other. In that case, γ_E can be expressed as $\gamma_E = \bar{\gamma}_E = \frac{r_E P_S}{N_0}$, and the SOP expression can be written as

$$P_{\rm SO} = \Pr[\gamma_B < \gamma_{th}(1+\gamma_E) - 1], \tag{25}$$

and it can be obtained as

$$P_{\rm SO} = \sum_{\rho=0}^{\infty} \binom{\alpha_B}{\rho} (-1)^{\rho} \exp\left[-\rho\left(\frac{\gamma_{th}(1+\bar{\gamma}_E)-1}{\eta_B^2\overline{\gamma}_B}\right)^{\frac{\beta_B}{2}}\right]. \tag{26}$$

B. PROBABILITY OF POSITIVE SECRECY

In PLS, E can be a licensed user of the system which has an intention of eavesdropping on the communication between A and B. In that case, A is aware of E and it has to satisfy positive secrecy capacity $C_s > 0$. Mathematically speaking, PPSC can be defined as [25]

$$\begin{aligned} P_{\rm PPSC} &= \Pr[C_s > 0] \\ &= \Pr\left[\log_2\left(1+\gamma_B\right) > \log_2(1+\gamma_E)\right], \end{aligned} \tag{27}$$

and it can be expressed as

$$P_{\rm PPSC} = 1 - \int_0^{\infty} F_{\gamma_B}(\gamma) f_{\gamma_E}(\gamma) d\gamma \tag{28}$$

For use-case 1 and use-case 2, PPSC can be obtained by invoking (21) and (23) into (28) as

$$\begin{aligned} P_{\rm PPSC} = 1 - &\frac{\alpha}{(\eta^2\overline{\gamma}_E)^{\frac{\beta}{2}}} \sum_{\rho=0}^{\infty}\sum_{k=0}^{\infty} \binom{\alpha}{\rho}\binom{\alpha-1}{k}(-1)^{\rho+k} \\ &\times \left((k+1)\left(\frac{1}{\eta^2\overline{\gamma}_E}\right) + \rho\left(\frac{1}{\eta^2\overline{\gamma}_B}\right)\right)^{-\frac{\beta}{2}}. \end{aligned} \tag{29}$$

For the third use-case, we can write PPSC as

$$\begin{aligned} P_{\rm PPSC} &= \Pr[C_s > 0] \\ &= \Pr\left[\log_2\left(1+\gamma_B\right) > \log_2(1+\gamma_E)\right] \\ &= \Pr\left[\gamma_B > \gamma_E\right] \\ &= 1 - \sum_{\rho=0}^{\infty}\binom{\alpha_B}{\rho}(-1)^{\rho}\exp\left[-\rho\left(\frac{\gamma_E}{\eta_B^2\overline{\gamma}_B}\right)^{\frac{\beta_B}{2}}\right]. \end{aligned} \tag{30}$$

C. AVERAGE SECRECY CAPACITY

For the first two use-cases, ASC can be found by averaging the secrecy capacity as

$$\bar{C}_s = E[C_s] = E[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)] \tag{31}$$

Next, we apply Jensen's inequality to ease the ASC expression. In Jensen's inequality, if X is a random variable and θ is a convex function, then $\theta E[X] \leq E[\theta X]$, $E[\cdot]$ denotes the Expectation-operation. If the above-given theorem is applied into (31) ASC can be expressed as

$$\bar{C}_s \approx \log_2(1+E[\gamma_B]) - \log_2(1+E[\gamma_E]), \tag{32}$$

and it can be obtained as

$$E[\gamma_j] = \int_0^{\infty} \gamma f_{\gamma_j}(\gamma) d\gamma \tag{33}$$

By substituting $f_{\gamma_j}(\gamma)$ into (33), $E[\gamma_j]$ can be expressed as can be seen in (34)

$$\begin{aligned} E[\gamma_j] = &\frac{\alpha_j\beta_j}{2(\eta_j^2\overline{\gamma}_j)^{\frac{\beta_j}{2}}} \sum_{k=0}^{\infty}\binom{\alpha_j-1}{k}(-1)^k \int_0^{\infty}\gamma^{\frac{\beta_j}{2}} \\ &\times \exp\left[-(k+1)\left(\frac{\gamma}{\eta_j^2\overline{\gamma}_j}\right)^{\frac{\beta_j}{2}}\right] d\gamma \end{aligned} \tag{34}$$

and the result can be obtained by using [24, eqn. (3.478.1)] as seen in (35).

$$\begin{aligned} E[\gamma_j] = &\frac{\alpha_j\beta_j}{2(\eta_j^2\overline{\gamma}_j)^{\frac{\beta_j}{2}}} \sum_{k=0}^{\infty}\binom{\alpha_j-1}{k}(-1)^k\left(\frac{2}{\beta_j}\right) \\ &\times\left((k+1)\left(\frac{1}{\eta_j^2\overline{\gamma}_j}\right)^{\frac{\beta_j}{2}}\right)^{-(1+2/\beta_j)} \Gamma\left(1+2/\beta_j\right), \end{aligned} \tag{35}$$

In (35), $\Gamma(\cdot)$ shows the Gamma function. By substituting (35) into (33) ASC can be obtained.

In the third use-case, we assume a turbulence-free communication model between A and E. Therefore, we can write ASC as

$$\begin{aligned} \bar{C}_s &= \left[\log_2\left(1+E\left[\gamma_B\right]\right) - \log_2\left(1+E[\gamma_E]\right)\right] \\ &\approx \left[\log_2\left(1+E\left[\gamma_B\right]\right) - \log_2\left(1+\frac{r_e P_S}{N_0}\right)\right], \end{aligned} \tag{36}$$

and $E[\gamma_B]$ can be obtained as given in (35).

D. SECRECY THROUGHPUT

ST presents another secrecy metric that is proposed to evaluate the overall efficiency of achieving reliable and secure communication [26]. Mathematically, ST can be obtained using the following expression

$$ST = R_s(1-P_{\rm SO}) \tag{37}$$

and therefore ST can be easily obtained by invoking (24) and (26) into the above equation for all use-cases.

E. DIVERSITY GAIN ANALYSIS

For the first two use-cases, when $\gamma_B \to \infty$, the $P_{\rm SO}^{\infty}$ can be expressed as

$$\int_0^{\infty} F_{\gamma_B}^{\infty}(\gamma\gamma_{th}) f_{\gamma_E}(\gamma) d\gamma, \tag{38}$$

where $F_{\gamma_B}^{\infty}(\gamma\gamma_{th})$ can be obtained by using the Taylor series expansion of $\exp[-ax]$ as

$$F_{\gamma_B}^{\infty}(\gamma\gamma_{th}) = \left(\frac{\gamma_{th}}{\eta_B^2\bar{\gamma}_B}\right)^{\frac{\beta_B\alpha_B}{2}} \tag{39}$$

By inserting (39) and (22) into (38), with the aid of [24, eqn. (3.478.1)] and after a few theoretical manipulations, asymptotic SOP can be expressed as

$$P_{\mathrm{SO}}^{\infty} = \frac{\alpha_E}{\left(\eta_E^2 \bar{\gamma}_E\right)^{\frac{\beta_E}{2}} \left(\eta_B^2 \bar{\gamma}_B\right)^{\frac{\beta_B \alpha_B}{2}}} \times \Gamma\left(1 + \frac{\beta_B \alpha_B}{\beta_E}\right) \times \sum_{t=0}^{\infty} \binom{\alpha_E - 1}{t} (-1)^t \left((t+1) \left(\frac{\gamma_{th}}{\eta_E^2 \bar{\gamma}_E} \right)^{\frac{\beta_E}{2}} \right)^{-\left(\frac{\beta_B \alpha_B}{\beta_E} + 1\right)}. \tag{40}$$

To obtain the diversity gain, we can express (40) as

$$P_{\mathrm{SO}}^{\infty} = \kappa \left(\frac{1}{\bar{\gamma}_B} \right)^{G_d}, \tag{41}$$

where κ is

$$\kappa = \frac{\alpha_E}{\left(\eta_E^2 \bar{\gamma}_E\right)^{\frac{\beta_E}{2}} \left(\eta_B^2\right)^{\frac{\beta_B \alpha_B}{2}}} \times \Gamma\left(1 + \frac{\beta_B \alpha_B}{\beta_E}\right) \times \sum_{t=0}^{\infty} \binom{\alpha_E - 1}{t} (-1)^t \left((t+1) \left(\frac{\gamma_{th}}{\eta_E^2 \bar{\gamma}_E} \right)^{\frac{\beta_E}{2}} \right)^{-\left(\frac{\beta_B \alpha_B}{\beta_E} + 1\right)}, \tag{42}$$

and diversity gain can be obtained as $G_d = \frac{\beta_B \alpha_B}{2}$.

For the third use-case, we can apply the Taylor series expansion at (26), and express the asymptotic SOP expression as

$$P_{\mathrm{SO}}^{\infty} = \left(\frac{\gamma_{th}(1 + \bar{\gamma}_E) - 1}{\eta_B^2 \bar{\gamma}_B} \right)^{\frac{\alpha_B \beta_B}{2}}, \tag{43}$$

and diversity gain can be obtained as $G_d = \frac{\beta_B \alpha_B}{2}$.

V. NUMERICAL RESULTS AND DISCUSSION

In this section, we analyze the secrecy performance of the proposed use-cases for different conditions. For all use-cases, we consider that all the HAPS nodes are positioned at an altitude of 19 km. For the third use-case, w assume that the LEO satellite is orbiting at an altitude of 500 km. For use-case 2, the height of the GS is 0.8 km above the mean sea level.

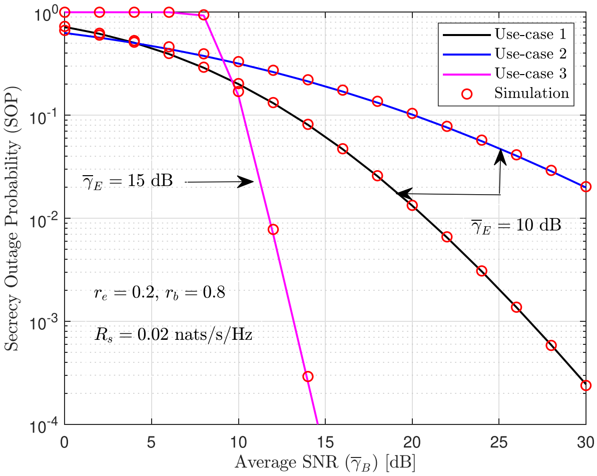

FIGURE 2. SOP performance of the proposed models vs. $\bar{\gamma}_B$.

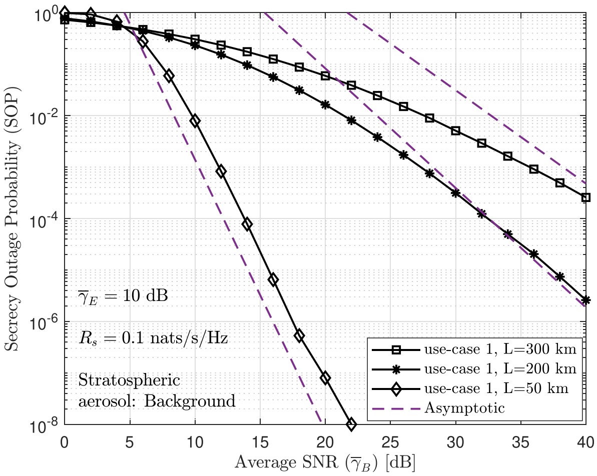

FIGURE 3. SOP performance of use-case 1 vs. $\bar{\gamma}_B$.

Fig. 2 depicts the SOP performance of the proposed system models with respect to the average SNR of the intended receiver $\bar{\gamma}_B$. For the two first use-cases the average SNR of the attacker is set to 10 dB. However, for the third use-case, as we assume the E is very close to A, we consider in that case a stronger SNR as 15 dB. For the HAPS-to-HAPS communication, we consider a distance of 200 km separating both nodes and the presence of background stratospheric attenuation. For both uplink communication scenarios, the zenith angle is set to $\zeta = 70°$. For all scenarios, the amount of leaked power of E is set to $r_e = 0.2$ and the secrecy rate is taken as $R_s = 0.02$ nats/s/Hz. As can be observed from the figure, at lower values of $\bar{\gamma}_B$, the HAPS-to-HAPS communication provides better security performance than other models. However, at higher SNR, the uplink satellite communication is more secure. This is due to the fact that when the attacker is next to the transmitter, fewer data can be captured, whereas, when E is located closer to the main receiver, more information can be leaked due to attenuation. In addition, as ground communication is more affected by atmospheric conditions, we can conclude that more optical beams can be reflected and thus received by attackers. Finally, it is clear from the figure that the theoretical results are in good agreement with the Monte Carlo (MC) simulations.

In Fig. 3, we examine the SOP performance of HAPS-to-HAPS communication for difference distances L_{H}. In this case, $\bar{\gamma}_E$ is set to 10 dB, $R_s = 0.1$ nats/s/Hz, and we assume the presence of background stratospheric aerosol. As can be seen from the figure, increasing the distance separating the HAPS nodes, deteriorates the secrecy performance. Specifically, as the distance increases, the fluctuations in the signal increases and thus the security performance decreases. Therefore, lower atmospheric attenuation enhances the communication security. To conclude, the secrecy performance is highly dependent on the atmospheric conditions. Finally, from this figure, we can observe that the exact SOP curves tend towards the asymptotic SOP results which are represented

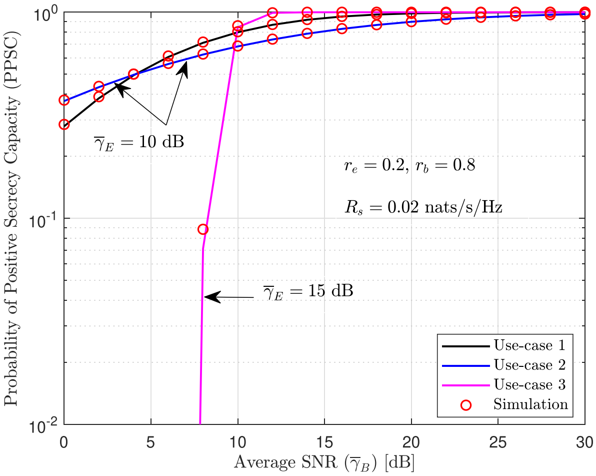

FIGURE 4. PPSC performance of the proposed models vs. $\overline{\gamma}_B$.

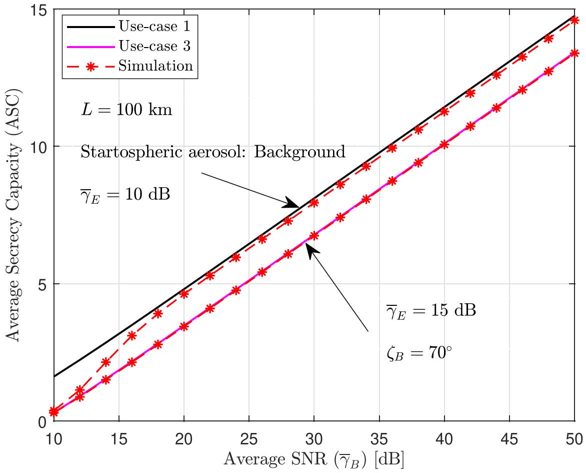

FIGURE 5. ASC performance of use-cases 1 and 3 vs. $\overline{\gamma}_B$.

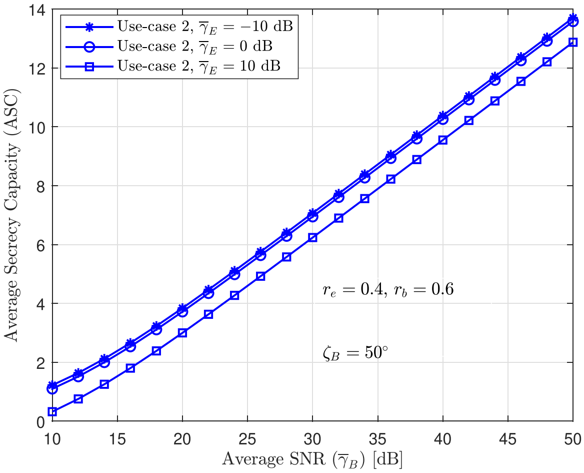

FIGURE 6. ASC performance of use-case 2 vs. $\overline{\gamma}_B$.

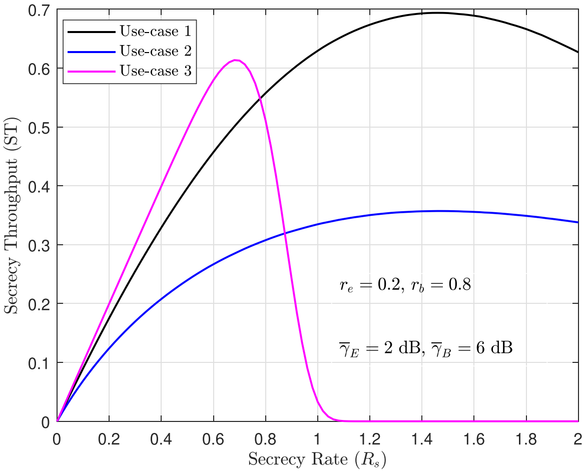

FIGURE 7. ST performance of the proposed models vs. R_s.

by dashed lines in the high SNR region, which verifies the accuracy of our derivations.

Fig. 4 evaluates the PPSC performance of the proposed models. For this figure, we assume the same conditions as Fig. 2. In this figure, we can see that the results agree well with MC simulations showing the effectiveness of our performance analysis. In addition, the figure shows that at low SNR values the HAP-LEO satellite uplink communication scenario is more susceptible to eavesdropping. As the average SNR of the intended receiver increases and exceeds the average SNR of the eavesdropper, the secrecy performance is significantly improved and he HAPS-LEO satellite uplink communication scenario shows better performance. Finally, the average SNR of the eavesdropper exhibit a significant impact on the secrecy performance.

Fig. 5 shows the ASC performance of use-cases 1 and 3. As can be seen from the figure, when decreasing the distance between the two HAPS nodes for use-case 1, the secrecy performance is enhanced and use-case 1 performs better than use-case 3. In fact, decreasing the communication distance decreases the scintillation index which imposes a lower level of fluctuations and thus improves the main channel capacity and the secrecy performance. Under these assumptions, different from Figs. 2 and 4, the scenario when E is positioned next to the main receiver achieves higher ASC. In addition, at higher SNR values $\overline{\gamma}_B$, we can see the good agreement with MC simulations.

Fig. 6 depicts the ASC performance for the ground to HAPS uplink scenario. The zenith angle is set to $\zeta = 50°$ and the amount of the leaked power to E is $r_e = 0.4$. As expected, increasing the average SNR of E deteriorates the overall secrecy performance. Therefore, $\overline{\gamma}_E$ has a direct impact on providing secure communication.

Fig. 7 shows the ST performance of the proposed use-cases versus the target secrecy rate R_s. In all scenarios, the average SNR of the eavesdropper $\overline{\gamma}_E$ is set to 2 dB and the average SNR of the intended receiver $\overline{\gamma}_E = 6$ dB. As can be seen in the figure, the ST goes up as R_s increases to a specific value and then decreases. This is brought on by ST's reliance on R_s. Specifically, when R_s is relatively low, ST rises. However, when R_s exceeds a particular threshold value, the system cannot guarantee reliability and security. In addition, the figure reveals that under these assumptions, for low values of R_s, the HAPS-LEO satellite uplink communication scenario provides better reliability and security. However, after a particular value, ST goes to zero and the HAPS to HAPS communication scenario becomes more secure and reliable.

A. DESIGN GUIDELINES

- In all use-cases, the results have shown that the fraction of the reflected beam that is gathered by the eavesdropper (r_e), the eavesdropper SNR, the altitude and position of the HAPS are of utmost importance for secure HAPS communications. For example, when $r_e > 0.5$, secure communication can not be established among the peers.
- Among three use-cases, the security of ground-to-HAPS communication is so critical as the optical beam can be scattered due to eddies and adverse weather conditions in the troposphere. This is why it can achieve only 10^{-1} SOP performance at 20 dB for $\bar{\gamma}_E = 10$ dB.
- In HAPS-to-HAPS communications, we observe that distance is of utmost importance as the leakage level increases with distance. Specifically, when $L >> 200$ km, the SOP performance decreases rapidly.
- Among all communication models, HAPS-to-satellite communication has a decent secrecy performance as E can not gather enough information due to its proximity to the transmitter side. In addition, the attenuation is so low in uplink HAPS-to-satellite communications.

VI. CONCLUSION

The integration of terrestrial and non-terrestrial networks is essential to provide flawless connectivity over the globe. This vision is consistent with the VHetNet architecture. The backbone of this network is the high altitude platform station (HAPS) systems. A HAPS node can provide reliable and ubiquitous connectivity among satellites, UAVs, and terrestrial users. In this architecture, the confidentiality of the information is very important. In this regard, we propose three different use-cases for optical HAPS eavesdropping and investigate the physical layer security performances by using SOP, PPSC, ASC, and ST analyses. The results have shown that eavesdropper SNR, the fraction of information scattered, zenith angle, and distance can be critical in optical HAPS systems for secure communication.

REFERENCES

[1] *3rd Gener. Partnership Project (3GPP)*, “Study on new radio (NR) to support non-terrestrial networks v15.4.0 (rel. 15),” 3GPP, Sophia Antipolis, France, Tech. Rep., 2020.

[2] G. K. Kurt et al., “A vision and framework for the high altitude platform station (HAPS) networks of the future,” *IEEE Commun. Surv. Tut.*, vol. 23, no. 2, pp. 729–779, Apr.–Jun. 2021.

[3] M. S. Alam, G. K. Kurt, H. Yanikomeroglu, P. Zhu, and N. D. Dào, “High altitude platform station based super macro base station constellations,” *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 103–109, Jan. 2021.

[4] Z. Yin et al., “UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2739–2751, Mar. 2022.

[5] F. A. d’Oliveira, F. C. L. D. Melo, and T. C. Devezas, “High-altitude platforms–present situation and technology trends,” *J. Aerosp. Technol. Manage.*, vol. 8, no. 3, pp. 249–262, 2016.

[6] O. Ben Yahia, E. Erdogan, and G. K. Kurt, “HAPS-assisted hybrid RF-FSO multicast communications: Error and outage analysis,” *IEEE Trans. Aerosp. Electron. Syst.*, early access, Jun. 24, 2020, doi: 10.1109/TAES.2022.3186296.

[7] A. Viswanath, V. K. Jain, and S. Kar, “Analysis of earth-to-satellite free-space optical link performance in the presence of turbulence, beam-wander induced pointing error and weather conditions for different intensity modulation schemes,” *IET Commun.*, vol. 9, no. 18, pp. 2253–2258, 2015.

[8] E. Erdogan, I. Altunbas, G. K. Kurt, and H. Yanikomeroglu, “Cooperation in space: HAPS-aided optical inter-satellite connectivity with opportunistic scheduling,” *IEEE Commun. Lett.*, vol. 26, no. 4, pp. 882–886, Apr. 2022.

[9] R. Swaminathan, S. Sharma, N. Vishwakarma, and A. S. Madhukumar, “HAPS-based relaying for integrated space–air–ground networks with hybrid FSO/RF communication: A performance analysis,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 3, pp. 1581–1599, Jun. 2021.

[10] Y. Shi, Y. Gao, and Y. Xia, “Secrecy performance analysis in internet of satellites: Physical layer security perspective,” in *Proc. IEEE/CIC Int. Conf. on Commun. China*, 2020, pp. 1185–1189.

[11] Z. Yin et al., “Secrecy rate analysis of satellite communications with frequency domain NOMA,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 11847–11858, Dec. 2019.

[12] Z. Yin, N. Cheng, T. H. Luan, and P. Wang, “Physical layer security in cybertwin-enabled integrated satellite-terrestrial vehicle networks,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4561–4572, May 2022.

[13] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, “Physical layer security framework for optical non-terrestrial networks,” in *Proc. IEEE 28th Int. Conf. Telecommun.*, 2021, pp. 162–166.

[14] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, “UAV-Enabled secure communications: Joint trajectory and transmit power optimization,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4069–4073, Apr. 2019.

[15] C. Wen, L. Qiu, and X. Liang, “Securing UAV communication with mobile UAV eavesdroppers: Joint trajectory and communication design,” in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2021, pp. 1–6.

[16] Q. Wu, W. Mei, and R. Zhang, “Safeguarding wireless network with UAVs: A physical layer security perspective,” *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[17] J. Sun, Z. Sheng, A. A. Nasir, H. Wei, Y. Fang, and A. H. Muqaibel, “Secure UAV-enabled OFDMA communications,” in *Proc. IEEE 94th Veh. Technol. Conf.*, 2021, pp. 01–05.

[18] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, “Optical satellite eavesdropping,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 10126–10131, Sep. 2022.

[19] ITU-R, “Prediction methods required for the design of Earth-space systems operating between 20 THz and 375 THz,” *Int. Telecommun. Union Recommendation P.1622*, 2003.

[20] R. B. Porras, “Exponentiated Weibull Fading Channel Model in Free-Space Optical Communications under Atmospheric Turbulence,” *Ph.D. dissertation, Dept. Signal Theory Commun., Univ. Politècnica de Catalunya (UPC)*, Barcelona, Spain, May 2013.

[21] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, Bellingham, WA, USA: SPIE Press, 2005.

[22] H. Lei, H. Luo, K.-H. Park, Z. Ren, G. Pan, and M.-S. Alouini, “Secrecy outage analysis of mixed RF-FSO systems with channel imperfection,” *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–13, Jun. 2018.

[23] E. Erdogan, “Joint user and relay selection for relay-aided RF/FSO systems over exponentiated Weibull fading channels,” *Opt. Commun.*, vol. 436, pp. 209–215, 2019.

[24] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic Press, 2014.

[25] E. Erdogan, I. Altunbas, G. K. Kurt, and H. Yanikomeroglu, “The secrecy comparison of RF and FSO eavesdropping attacks in mixed RF-FSO relay networks,” *IEEE Photon. J.*, vol. 14, no. 1, pp. 1–8, Feb. 2022.

[26] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, “Optimization of code rates in SISOME wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.