Optical Satellite Eavesdropping

Olfa Ben Yahia, *Graduate Student Member, IEEE*,
Eylem Erdogan, *Senior Member, IEEE*,
Gunes Karabulut Kurt, *Senior Member, IEEE*,
Ibrahim Altunbas, *Senior Member, IEEE*,
and Halim Yanikomeroglu, *Fellow, IEEE*

***Abstract*—In recent years, satellite communication (SatCom) systems have been widely used for navigation, broadcasting application, disaster recovery, weather sensing, and even spying on the Earth. As the number of satellites is highly increasing and with the radical revolution in wireless technology, eavesdropping on SatCom will be possible in next-generation networks. In this context, we introduce the satellite eavesdropping approach, where an eavesdropping spacecraft can intercept optical communications established between a low Earth orbit satellite and a high altitude platform station (HAPS). Specifically, we propose two practical eavesdropping scenarios for satellite-to-HAPS (downlink) and HAPS-to-satellite (uplink) optical communications, where the attacker spacecraft can eavesdrop on the transmitted signal or the received signal. To quantify the secrecy performance of the scenarios, the average secrecy capacity and secrecy outage probability expressions are derived and validated with Monte Carlo simulations. Moreover, the secrecy throughput of the proposed models is investigated. We observe that turbulence-induced fading significantly impacts the secrecy performance of free-space optical communication.**

***Index Terms*—Free-space optical, high altitude platform station, physical layer security, satellite eavesdropping.**

I. Introduction

Over the past few years, an explosion in demand for high data rates has precipitated the integration of non-terrestrial networks with terrestrial infrastructure. In fact, three layers of heterogeneous networks are considered for state-of-the-art next-generation wireless communications. The well-known vertical heterogeneous network (VHetNets) architecture is composed of a space network, an aerial network, and a terrestrial network [1]. In this architecture, low Earth orbit (LEO) satellites, which orbit at altitudes of less than 2,000 km, have attracted broad interest from researchers. LEO satellites are expected to be the key enabler of the space layer in future wireless networks due to their potential to provide real-time communication with enhanced data rates and high coverage.

Two interacting sub-layers are envisioned as part of the aerial network layer. As described in [2], one sub-layer would be composed of unmanned aerial vehicle (UAV) nodes, and the second sub-layer would include high altitude platform station (HAPS) systems. A HAPS is defined as an aircraft positioned in the stratosphere at an altitude between 17-22 km. These platforms may be airships, airplanes, or balloons [3]. HAPS provides a number of advantages over terrestrial networks in terms of higher capacity, better propagation performance, enhanced coverage, lower costs, and a better quality of service [4].

To connect all the elements of VHetNets architecture and provide broad coverage with high data rates, free-space optical (FSO) communication is an important enabler. FSO communication provides an efficient way of transmitting data through free space with the use of laser beams. Benefits of FSO communication include high bandwidth, unlicensed spectrum, low power requirements, and better security [5]. However, FSO links are affected by scintillation, pointing errors, and beam wander can be effective in uplink (UL) optical communication [6].

One major challenge in non-terrestrial networks is to guarantee a secure exchange of information. Typically, communication security is guaranteed through encryption. In recent research, however, physical layer security (PLS) has been considered a relevant solution complementary to cryptographic-based schemes to secure information against eavesdroppers relying on channel characteristics [7]. Lately, PLS has been introduced for FSO communication. In FSO communication, the eavesdropper should be positioned very close to the communicating peers, so that it can capture the beam that is reflected by the aerosols or gases in the atmosphere. However, if the eavesdropper blocks the laser beam while intercepting the information, the receiver can notice the leakage of power and thus stop communication for security issues. An alternative scenario can occur when misalignment arises between the communicating peers due to severe pointing errors or diffraction. In such case, the beam spreads out and the eavesdropper may receive the refracted beam [8]. Even though optical communication can be intercepted, only a few papers have considered PLS performance. Y. Ai *et al.* [9] discussed the PLS performance of three realistic scenarios by assuming different eavesdropper locations. It was shown that atmospheric condition imposes less impact on the secrecy performance when the eavesdropper is placed near the transmitter. In [10], the cases in which the eavesdropper is placed in proximity to the receiver or in proximity to the transmitter are investigated. It was observed that when the eavesdropper is close to the legitimate transmitter, it can easily intercept the communication by taking advantage of the larger attenuation affecting the signal when propagating through the FSO channel. In [11], the authors derived the closed-form expressions of average secrecy capacity (ASC), secrecy outage probability (SOP), and strictly positive secrecy capacity (SPSC) over Málaga atmospheric turbulence channels in the presence of pointing errors for conventional optical communications. Furthermore, [12] evaluated the impact of an eavesdropper's position on the secrecy performance of terrestrial FSO systems. In particular, the closed-form expressions of the outage secrecy capacity and SPSC for PLS performance are derived. The authors in [13] studied the PLS performance of FSO communication in terms of a recently proposed metric named effective secrecy throughput. Furthermore, under generalized misalignments and atmospheric turbulence conditions, the authors in [14] studied the ASC for the log-normal fading model. Similar to RF communication, it was shown that channel correlation is crucial for secrecy capacity in all scenarios. The threat introduced by an eavesdropping spacecraft has not yet been investigated in the literature.

For decades, satellites have been valuable for politics and military purposes. Known as "eyes in the sky", reconnaissance satellites have

Manuscript received 3 December 2021; revised 1 April 2022; accepted 10 May 2022. Date of publication 20 May 2022; date of current version 19 September 2022. This work was supported in part by the National Sciences and Engineering Research Council's Discovery Grant. The review of this article was coordinated by Dr. Chau Yuen. *(Corresponding author: Olfa Ben Yahia.)*

Olfa Ben Yahia and Ibrahim Altunbas are with the Department of Electronics and Communication Engineering, Istanbul Technical University, 34467 Istanbul, Turkey (e-mail: yahiao17@itu.edu.tr; ibraltunbas@itu.edu.tr).

Eylem Erdogan is with the Department of Electrical and Electronics Engineering, Istanbul Medeniyet University, 34720 Istanbul, Turkey (e-mail: eylem.erdogan@medeniyet.edu.tr).

Gunes Karabulut Kurt is with the Department of Electrical Engineering, Polytechnique Montréal, Montréal, QC H3T1J4, Canada (e-mail: gunes.kurt@polymtl.ca).

Halim Yanikomeroglu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON 2K1S5B6, Canada (e-mail: halim@sce.carleton.ca).

Digital Object Identifier 10.1109/TVT.2022.3176119

been orbiting the Earth for more than 40 years [15]. Specifically, surveying the Earth from space is an effective strategy in wars and gathering information about other countries [15]. With the revolution in space technology, we highlight the idea of eavesdropping on satellites for next-generation networks. To the best of the authors' knowledge, this threat has not yet been studied in the literature.

The current literature demonstrates a growing interest in security issues for FSO communication systems. However, these works are limited to optical terrestrial communications. Only [16] investigated the optical eavesdropping in non-terrestrial networks by considering both HAPS and UAV eavesdropping. Motivated by the significant gap in PLS performance for optical communications in non-terrestrial networks, we make the following contributions:

- We introduce a new approach for optical satellite eavesdropping, where a spacecraft is eavesdropping on an LEO satellite.
- We investigate the secrecy performance of optical communication under two realistic scenarios. At first, we assume a downlink (DL) communication between an LEO satellite and a HAPS node. Secondly, we consider a UL communication from the HAPS to the satellite. In both cases, we assume that the external observer (eavesdropper spacecraft), which intends to intercept the communication, is located very close to the satellite, within the convergence area of its optical beam.
- We study the impact of power leakage and adverse stratospheric conditions on secrecy performance.
- We obtain novel closed-form expressions of the secrecy outage probability (SOP) and average secrecy capacity (ASC) for exponentiated Weibull (EW) fading while considering the amount of power captured by the eavesdropping spacecraft. In addition, secrecy throughput (ST) analysis is provided.

The remainder of the paper is organized as follows. Channels and system models are presented in Section II. In Section III, the secrecy performance expressions are provided. Numerical results are outlined in Section IV followed by a related discussion. Finally, Section V concludes the paper.

II. Channels and System Model

In this paper, we propose a novel scenario of eavesdropping attacks in space. As shown in Fig. 1, we assume an LEO satellite S that communicates with a HAPS $\mathcal{H}$ node in the presence of sophisticated eavesdropping spacecraft E located very close to S. We first consider S to $\mathcal{H}$ DL communication, where E is within the convergence area of the optical beam of S so that it can eavesdrop on the transmitted beam. Secondly, we consider $\mathcal{H}$ to S UL communication, where E tries to capture the $\mathcal{H}$'s information. Due to the HAPS node's quasi-stationary position, tracking and accuracy issues, and the Doppler shift can be tolerated for the communication between S and $\mathcal{H}$. In both scenarios, E can capture only a small fraction r_e of the transmitted signal, whereas the intended receiver collects more power resulting in a fraction r_b, where $r_e + r_b \leq 1$. Note that the parameters r_b and r_e depend on the aperture size of each device along with the beam divergence angle. In the analysis, we assume that the locations of satellite, HAPS, and eavesdropper spacecraft can be used to extract the channel's physical model, which is representative of the channel state information [17].

For S to $\mathcal{H}$ communication scenario, the received signal at $\mathcal{H}$ can be given as $y_{\mathcal{H}} = \sqrt{r_b P_S} I_{\mathcal{H}} x_S + n_{\mathcal{H}}$, and for $\mathcal{H}$ to S communication, the received signal at S can be written similarly as $y_S = \sqrt{r_b P_{\mathcal{H}}} I_S x_{\mathcal{H}} + n_S$. For both scenarios, the received signals at E sent by node j, $j \in \{S, \mathcal{H}\}$ can be written as $y_E = \sqrt{r_e P_j} I_E x_j + n_E$. P_S, $P_{\mathcal{H}}$ denote the transmit power of S and $\mathcal{H}$ respectively, $I_{\mathcal{H}}$, I_S, I_E indicate the received irradiance at $\mathcal{H}$, S, and E respectively. x_S, $x_{\mathcal{H}}$ are the transmitted symbols with unit energy, and $n_{\mathcal{H}}$, n_S indicate the additive white Gaussian noise (AWGN) with one-sided noise power spectral density N_0. Thus, the instantaneous signal-to-noise ratio (SNR) at $\mathcal{H}$ can be given as

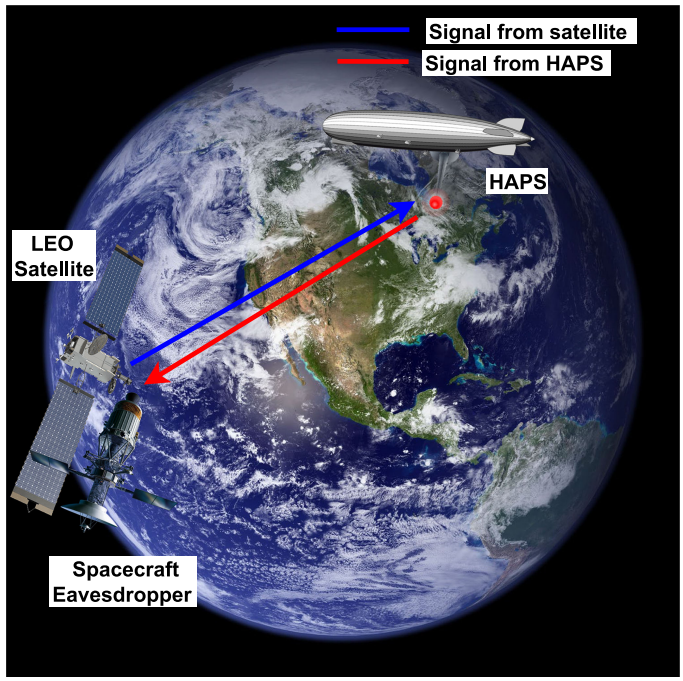

Fig. 1. Illustration of the satellite eavesdropping.

$$\gamma_{\mathcal{H}} = \frac{r_b P_S}{N_0} I_{\mathcal{H}}^2 = \overline{\gamma}_{\mathcal{H}} I_{\mathcal{H}}^2, \tag{1}$$

where $\overline{\gamma}_{\mathcal{H}} = \frac{r_b P_S}{N_0}$ defines the average SNR at $\mathcal{H}$ with $\mathbb{E}[I_{\mathcal{H}}^2] = 1$, and the instantaneous SNR at S and E can be expressed similarly after changing the subscripts as $\gamma_S = \frac{r_b P_{\mathcal{H}}}{N_0} I_S^2 = \overline{\gamma}_S I_S^2$ and $\gamma_E = \frac{r_e P_j}{N_0} I_E^2 = \overline{\gamma}_E I_E^2$ with $\mathbb{E}[I_E^2] = \mathbb{E}[I_S^2] = 1$. We assume that the turbulence-induced fading follows EW distribution. EW fading has been shown to be the best fit for various aperture diameters for weak-to-strong turbulence levels, especially when aperture averaging is used to mitigate the impacts of turbulence and increase overall performance [18]. Hence, the probability density function (PDF) of the irradiance I for node k where $k \in \{S, \mathcal{H}, E\}$ is expressed as in [18,eqn. 11]. Furthermore, the cumulative distribution function (CDF) of γ_k can be expressed as [19, eqn. 9]

$$F_{\gamma_k}(\gamma) = \sum_{\rho=0}^{\infty} \binom{\alpha_k}{\rho} (-1)^{\rho} \exp\left[-\rho \left(\frac{\gamma}{\eta_k^2 \overline{\gamma}_k}\right)^{\frac{\beta_k}{2}}\right], \tag{2}$$

where α_k, β_k, and η_k indicate the shape parameters and the scale parameter, respectively, which depend on the scintillation index [18]. For the DL communication, the scintillation index $\sigma_{I_{DL}}^2$ at $\mathcal{H}$ can be written as

$$\sigma_{I_{DL}}^2 = \exp\left[\frac{0.49\sigma_R^2}{(1 + 1.11\sigma_R^{\frac{12}{5}})^{\frac{7}{6}}} + \frac{0.51\sigma_R^2}{(1 + 0.69\sigma_R^{\frac{12}{5}})^{\frac{5}{6}}}\right] - 1, \tag{3}$$

where σ_R^2 denotes the Rytov variance given in [17, Section (12)], and it depends on the zenith angle $\xi_{\mathcal{H}}$ and the wind speed $w_{\mathcal{H}}$. In UL communication, beam wander induced-pointing error has to be taken into consideration [20]. Therefore, the scintillation index $\sigma_{I_{UL}}^2$ can be written as

$$\sigma_{I_{UL}}^2 = 5.95(H_p - h_0)^2 \sec^2(\xi_p)\left(\frac{2W_0}{r_0}\right)^{\frac{5}{3}}\left(\frac{\alpha_{pe}}{W_p}\right)^2 + \exp\left[\frac{0.49\sigma_{Bu}^2}{(1+(1.11+\Theta)\sigma_{Bu}^{\frac{12}{5}})^{\frac{7}{6}}} + \frac{0.51\sigma_{Bu}^2}{(1+0.69\sigma_{Bu}^{\frac{12}{5}})^{\frac{5}{6}}}\right] - 1, \tag{4}$$

where H_p is the height of S and E, h_0 is the HAPS altitude, and ξ_p is the zenith angle for UL communication. W_0 is the beam radius at $\mathcal{H}$, the Fried's parameter r_0 depends on the wind speed w_p, α_{pe} indicates the beam wander-induced pointing errors variance, W_p is the beam size at S and E, and σ_{Bu}^2 is the Rytov variance in UL communication [20].

III. Secrecy Analysis

In this section, we analyze the secrecy performance of the proposed model. More specifically, the closed-form expressions of ASC, SOP, and ST are derived for both scenarios. According to the information-theoretic definition, the secrecy capacity C_s is the maximum achievable secrecy rate that can be expressed as follows [21]:

$$C_s = \begin{cases} \log_2(1+\gamma_j) - \log_2(1+\gamma_E)\,, \gamma_j > \gamma_E \\ 0\,, \text{otherwise}, \end{cases} \tag{5}$$

where γ_j denotes the instantaneous SNR of the main receiver.

A. Average Secrecy Capacity

In the context of PLS, ASC is an important metric for evaluating the secrecy performance of active eavesdropping.

1) Eavesdropping in Downlink Communication: In S to $\mathcal{H}$ DL communication, we assume that E is positioned very close to S. Therefore, the turbulence-induced fading can be neglected to provide a realistic model [10]. Thus, ASC for DL eavesdropping can be obtained by averaging the C_s as

$$\overline{C}_s = \frac{1}{\ln(2)}\mathbb{E}\left[\ln(1+\gamma_{\mathcal{H}}) - \ln(1+\gamma_E)\right]. \tag{6}$$

By using Jensen's inequality, for high SNR values, the ASC becomes

$$\overline{C}_s \cong \frac{1}{\ln(2)}\left[\ln\left(1+\mathbb{E}\left[\gamma_{\mathcal{H}}\right]\right) - \ln\left(1+\mathbb{E}[\gamma_E]\right)\right] \cong \frac{1}{\ln(2)}\left[\ln\left(1+\frac{r_b P_S}{N_0}\right) - \ln\left(1+\frac{r_e P_S}{N_0}\right)\right]. \tag{7}$$

2) Eavesdropping in Uplink Communication: In UL communication, we take the turbulence-induced fading into consideration. Thereby, $\overline{C}_s$ can be expressed as [22]

$$\overline{C}_s = \frac{1}{\ln(2)}\int_0^\infty \frac{F_{\gamma_E}(\gamma)}{1+\gamma}\left[1 - F_{\gamma_j}(\gamma)\right]d\gamma. \tag{8}$$

By substituting $F_{\gamma_E}(\gamma)$ and $F_{\gamma_j}(\gamma)$ in (8), the ASC for UL communication becomes

$$\overline{C}_s = \sum_{\rho=0}^{\infty}\binom{\alpha_E}{\rho}(-1)^\rho \int_0^\infty \frac{1}{1+\gamma}\exp\left[-\rho\left(\frac{\gamma}{\eta_E^2\overline{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right]d\gamma - \sum_{\rho=0}^{\infty}\sum_{t=0}^{\infty}(-1)^\rho(-1)^t\binom{\alpha_E}{\rho}\binom{\alpha_S}{t}\int_0^\infty \frac{1}{1+\gamma} \times \exp\left[-\left(\rho\left(\frac{\gamma}{\eta_E^2\overline{\gamma}_E}\right)^{\frac{\beta_E}{2}} + t\left(\frac{\gamma}{\eta_S^2\overline{\gamma}_S}\right)^{\frac{\beta_S}{2}}\right)\right]d\gamma. \tag{9}$$

In $\mathcal{H}$ to S communication, E should be located very close to the main receiver's photo aperture to gather some of the reflected signals due to atmospheric pressure or misalignment caused by the pointing errors. Thus, we assume that E encounters the same fading conditions as the intended receiver. Based on this assumption, we assume that $\beta_S = \beta_E = \beta$, $\alpha_S = \alpha_E = \alpha$, and $\eta_S = \eta_E = \eta$. Thereafter, using the following transformations $(1+x)^a = \frac{1}{\Gamma(-a)}G_{1,1}^{1,1}(x|\begin{smallmatrix} a+1 \\ 0 \end{smallmatrix})$, where $G_{p,q}^{m,n}(x\,|\begin{smallmatrix} a_1,\ldots,a_p \\ b_1,\ldots,b_q \end{smallmatrix})$ denotes the Meijer G-function, and $\exp(-bx) = G_{0,1}^{1,0}(bx|\begin{smallmatrix} - \\ 0 \end{smallmatrix})$ into (9), and by changing the variables as $X = \rho(\frac{\gamma}{\eta^2\overline{\gamma}_E})^{\frac{\beta}{2}}$, and with the aid of [23, eqn. 07.34.21.0013.01], the final expression of ASC can be formulated as in (10) given at the bottom of this page. In (10), the constants A and B are given as $A = (\frac{1}{\eta^2\overline{\gamma}_E})^{\frac{\beta}{2}}$, $B = (\frac{1}{\eta^2\overline{\gamma}_S})^{\frac{\beta}{2}}$, and $Y = \gamma^{\frac{\beta}{2}}(\rho A + tB)$.

B. Secrecy Outage Probability

Another important metric in PLS is SOP, which is the best fit for the scenario of passive eavesdropping, where the source does not have

$$\overline{C}_s = \frac{1}{\ln 2}\sum_{\rho=0}^{\infty}\binom{\alpha}{\rho}(-1)^\rho\frac{2}{\beta}\eta^2\overline{\gamma}_E\left(\frac{1}{\rho}\right)^{\frac{2}{\beta}}\int_0^\infty X^{\frac{2}{\beta}-1}G_{1,1}^{1,1}\left(\eta^2\overline{\gamma}_E\left(\frac{X}{\rho}\right)^{\frac{2}{\beta}}\middle|\begin{matrix}0\\0\end{matrix}\right)\times G_{0,1}^{1,0}\left(X\middle|\begin{matrix}-\\0\end{matrix}\right)dX$$
$$- \frac{1}{\ln 2}\sum_{\rho=0}^{\infty}\sum_{t=0}^{\infty}(-1)^{\rho+t}\binom{\alpha}{\rho}\binom{\alpha}{t}\frac{2}{\beta}\left(\frac{1}{\rho A+tB}\right)^{\frac{2}{\beta}}\int_0^\infty Y^{\frac{2}{\beta}-1}G_{1,1}^{1,1}\left(\left(\frac{Y}{\rho A+tB}\right)^{\frac{2}{\beta}}\middle|\begin{matrix}0\\0\end{matrix}\right)\times G_{0,1}^{1,0}\left(Y\middle|\begin{matrix}-\\0\end{matrix}\right)dY$$
$$= \frac{1}{\ln 2}\frac{2\times 2^{\frac{2}{\beta}-\frac{1}{2}}}{(2\pi)^{\beta-\frac{1}{2}}}\eta^2\overline{\gamma}_S\sum_{t=1}^{\infty}\binom{\alpha}{t}(-1)^{t+1}\left(\frac{1}{t}\right)^{\frac{2}{\beta}}G_{\beta+2,\beta}^{\beta,\beta+2}\left(4\times\left(\frac{\eta^2\overline{\gamma}_S}{t^{\frac{2}{\beta}}}\right)^\beta\middle|\begin{matrix}\Delta(\beta,0),\frac{1-(2/\beta)}{2},\frac{2-(2/\beta)}{2}\\ \Delta(\beta,0)\end{matrix}\right) - \frac{1}{\ln 2}\frac{2\times 2^{\frac{2}{\beta}-\frac{1}{2}}}{(2\pi)^{\beta-\frac{1}{2}}}$$
$$\times\sum_{\rho=1}^{\infty}\sum_{t=1}^{\infty}\binom{\alpha}{\rho}\binom{\alpha}{t}(-1)^{\rho+t+2}\left(\frac{1}{\rho A+tB}\right)^{\frac{2}{\beta}}G_{\beta+2,\beta}^{\beta,\beta+2}\left(4\times\left(\frac{1}{\rho A+tB}\right)^2\middle|\begin{matrix}\Delta(\beta,0),\frac{1-(2/\beta)}{2},\frac{2-(2/\beta)}{2}\\ \Delta(\beta,0)\end{matrix}\right) \tag{10}$$

any information about E. More specifically, SOP occurs when C_s falls below a predefined secrecy rate R_s. Therefore SOP can be expressed as $P_{\text{SO}} = \Pr[C_s \leq R_s]$.

1) Eavesdropping in Downlink Communication: As mentioned above, in DL communication, E is located very close to S and the SOP expression can be written as

$$\begin{aligned} P_{\text{SO}} &= \Pr[\gamma_{\mathcal{H}} \leq 2^{R_s} + 2^{R_s}\overline{\gamma}_E - 1] \\ &= F_{\gamma_{\mathcal{H}}}(2^{R_s} + 2^{R_s}\overline{\gamma}_E - 1). \end{aligned} \tag{11}$$

Thereby, by using (11) P_{SO} can be obtained as

$$P_{\text{SO}} = \sum_{\rho=0}^{\infty} \binom{\alpha_{\mathcal{H}}}{\rho} (-1)^{\rho} \exp\left[-\rho \left(\frac{2^{R_s} + 2^{R_s}\overline{\gamma}_E - 1}{\eta_{\mathcal{H}}^2 \overline{\gamma}_{\mathcal{H}}} \right)^{\frac{\beta_{\mathcal{H}}}{2}} \right]. \tag{12}$$

2) Eavesdropping in Uplink Communication: For UL communication, since we take into account turbulence-induced fading, the expression SOP can be written as [24]

$$\begin{aligned} P_{\text{SO}} &= \int_0^{\infty} F_{\gamma_j}\left(\gamma\gamma_{th} + \gamma_{th} - 1\right) f_{\gamma_E}(\gamma)\, d\gamma \\ &\simeq \int_0^{\infty} F_{\gamma_j}\left(\gamma\gamma_{th}\right) f_{\gamma_E}(\gamma)\, d\gamma. \end{aligned} \tag{13}$$

Thus, for UL eavesdropping, the SOP is expressed on the basis of (13), where the PDF of γ_E can be derived from (2) with respect to γ as

$$\begin{aligned} f_{\gamma_E}(\gamma) = &\frac{\alpha_E \beta_E \gamma^{\frac{\beta_E}{2}-1}}{2(\eta_E^2 \overline{\gamma}_E)^{\frac{\beta_E}{2}}} \sum_{q=0}^{\infty} \binom{\alpha_E - 1}{q} (-1)^q \\ &\times \exp\left[-(q+1) \left(\frac{\gamma}{\eta_E^2 \overline{\gamma}_E} \right)^{\frac{\beta_E}{2}} \right]. \end{aligned} \tag{14}$$

Then, by substituting (2) and (14) into (13), we obtain (15), given at the bottom of this page.

Finally, after some mathematical derivations and by using [25, 3.478.1], the final expression of SOP can be written as

$$\begin{aligned} P_{\text{SO}} = &\frac{\alpha}{(\eta^2 \overline{\gamma}_E)^{\frac{\beta}{2}}} \sum_{\rho=0}^{\infty} \binom{\alpha}{\rho} (-1)^{\rho} \sum_{q=0}^{\infty} \binom{\alpha - 1}{q} (-1)^q \\ &\times \left(\rho \left(\frac{\gamma_{th}}{\eta^2 \overline{\gamma}_S} \right) + (q+1) \left(\frac{1}{\eta^2 \overline{\gamma}_E} \right) \right)^{-\frac{\beta}{2}}. \end{aligned} \tag{16}$$

C. Secrecy Throughput

Another metric to evaluate the secrecy performance of the proposed system is ST [26]. This metric is exploited to characterize the overall efficiency of achieving reliable and secure transmission [27]. Mathematically, it can be written as

$$ST = R_s(1 - P_{\text{SO}}). \tag{17}$$

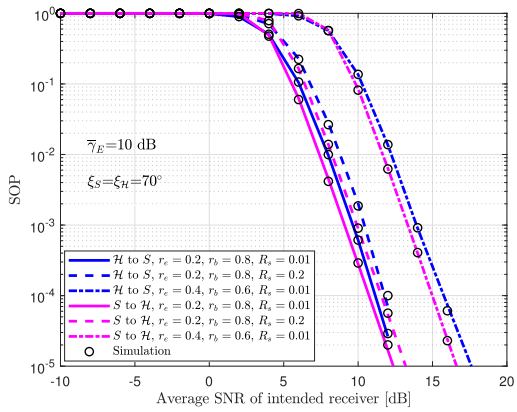

Fig. 2. SOP performance of the proposed scenarios for different fractions of received power and different secrecy rate when $\overline{\gamma}_E = 10$ dB.

The expressions of ST for uplink and downlink communication can be easily obtained by substituting (12) and (16) in (17).

IV. Numerical Results and Discussion

In this section, we evaluate the secrecy performance of satellite eavesdropping for the proposed models. For both scenarios, we consider the same parameters. The LEO satellite orbits at an altitude of 500 km, while the HAPS is located at 18 km. The zenith angles are set to $\xi_S = \xi_{\mathcal{H}} = 70^{\circ}$, the wind speed is given as $w_S = w_{\mathcal{H}} = 65$ m/s as we consider non-static stratospheric winds, and the secrecy rate is set as $R_s = 0.01$ bit/s/Hz for SOP simulations.

In Fig. 2, the SOP performance for both scenarios is plotted as a function of the SNR of the legitimate receiver. The eavesdropping average SNR is set to $\overline{\gamma}_E = 10$ dB. As we can see, the secrecy performance of the S to $\mathcal{H}$ communication is slightly better than that of $\mathcal{H}$ to S communication. This can be explained by the fact that when the illegitimate receiver approaches the receiver, it can collect more information as more beams can be reflected due to the greater distance. Moreover, for both scenarios, we can observe that the performance decreases as the fraction of the leaked power r_e received by the eavesdropper increases. Furthermore, as shown in the figure, increasing the secrecy rate R_s deteriorates the SOP performance. In addition, we can see the agreement of the theoretical expressions with the MC simulations.

In Fig. 3, we see the ASC performance for both scenarios. As the Fig. shows, by increasing the average SNR of the eavesdropper $\overline{\gamma}_E$ or decreasing the amount of power captured by the legitimate receiver, the overall secrecy performance degrades. Furthermore, for the S to $\mathcal{H}$ communication, we assume that the eavesdropper has a stronger SNR, as it is located very close to the LEO satellite and does not experience turbulence-induced fading effects. Additionally, it is clear from the Figure that the analytical expressions match exactly with the

$$\begin{aligned} P_{\text{SO}} &= \int_0^{\infty} \frac{\alpha_E \beta_E \gamma^{\frac{\beta_E}{2}-1}}{2(\eta^2 \overline{\gamma}_E)^{\frac{\beta_E}{2}}} \sum_{\rho=0}^{\infty} \sum_{q=0}^{\infty} \binom{\alpha_S}{\rho} \binom{\alpha_E - 1}{q} (-1)^{q+\rho} \exp\left[-\rho \left(\frac{\gamma\gamma_{th}}{\eta_S^2 \overline{\gamma}_S} \right)^{\frac{\beta_S}{2}} \right] \exp\left[-(q+1) \left(\frac{\gamma}{\eta_E^2 \overline{\gamma}_E} \right)^{\frac{\beta_E}{2}} \right] d\gamma \\ &= \frac{\alpha\beta}{2(\eta^2 \overline{\gamma}_E)^{\frac{\beta}{2}}} \sum_{\rho=0}^{\infty} \sum_{q=0}^{\infty} \binom{\alpha}{\rho} \binom{\alpha - 1}{q} (-1)^{q+\rho} \int_0^{\infty} \gamma^{\frac{\beta}{2}-1} \exp\left[-\left(\rho \left(\frac{\gamma_{th}}{\eta^2 \overline{\gamma}_S} \right)^{\frac{\beta}{2}} + (q+1) \left(\frac{1}{\eta^2 \overline{\gamma}_E} \right)^{\frac{\beta}{2}} \right) \gamma^{\frac{\beta}{2}} \right] d\gamma \end{aligned} \tag{15}$$

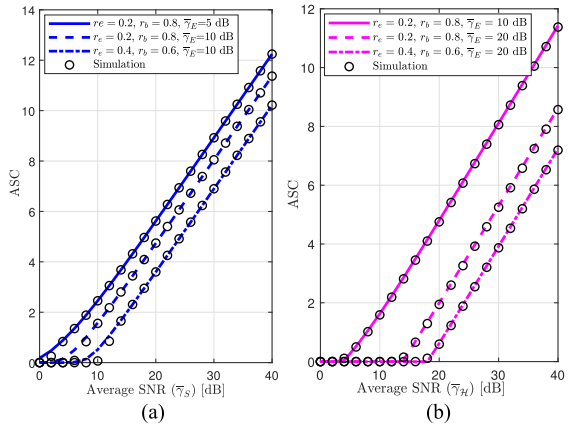

Fig. 3. ASC performance of both scenarios for different $\overline{\gamma}_E$ and different fractions of received power.

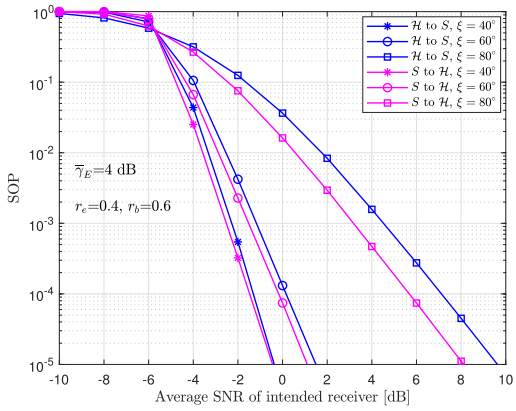

Fig. 4. SOP performance of the proposed models under different zenith angles, $\overline{\gamma}_E = 4$ dB.

MC simulations. Finally, we can observe that perfect secrecy is achieved when the average SNR of the intended receiver is higher than the SNR of the eavesdropper.

Fig. 4 shows the impact of the zenith angle on the proposed satellite eavesdropping scenarios. We set $\overline{\gamma}_E = 4$ dB and the fraction of power received by E as $r_e = 0.1$. As we can see, increasing the zenith angle decreases the amount of information that is captured by the legitimate receiver and leaked to the eavesdropper. Furthermore, the fluctuation in the signal is significant for a higher zenith angle. Thus, we conclude that there is a huge loss of performance. Moreover, as seen in the figure, for the lower zenith angles, the SOP performance is almost the same for both scenarios, and the simulation results reveal that the scintillation indexes are equal. However, when increasing the zenith angle to 80°, we can see a 2 dB difference between the two curves. Also, the impact of beam wander increases by increasing the zenith angle.

Fig. 5 evaluates the ST versus the target secrecy rate R_s for the proposed models for different average SNR levels of the intended receiver. In all cases, the average SNR of the spacecraft is set to 2 dB. As can be observed, the ST increases as R_s increases to a certain value and then decreases. This is due to the dependency of ST on R_s. The ST increases when the R_s is relatively low. However, when R_s exceeds a particular threshold value, the system cannot afford reliability and security. Furthermore, it is observed that the S to $\mathcal{H}$ downlink communication performs slightly better than $\mathcal{H}$ to S uplink

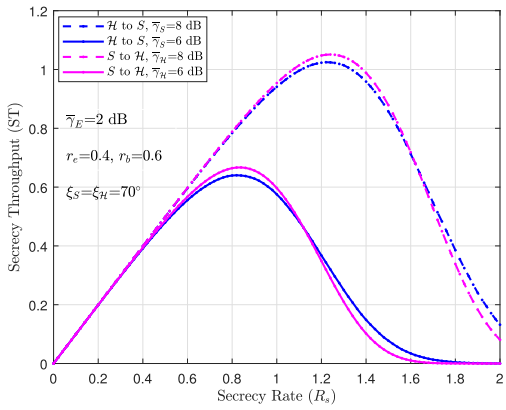

Fig. 5. ST performance of the proposed models vs. R_s.

scenario at lower R_s. However, after a particular value of R_s, the uplink scenario outperforms the downlink communication. Finally, as expected, increasing the average SNR of the intended receiver improves the ST performance.

Our main observations from the numerical results can be summarized as follows:

- Increasing the zenith angle between the HAPS node and the satellite decreases the overall performance.
- In the UL scenario, the eavesdropper spacecraft can collect more information as more beams can be reflected due to the greater distance.
- The fluctuations in the signal caused by atmospheric conditions have a direct impact on the secrecy performance.
- The SNR of the eavesdropper and the amount of power leaked to the eavesdropper are critical parameters to provide secure communication.
- From ST's point of view, it is observed that the system reliability and secrecy are compromised after a certain value of secrecy rate R_s.

These observations can be used to provide practical insights into the system architecture, so that a system designer can get a quick idea about the overall system performance, especially, as we are considering random channel characteristics.

V. Conclusion and Future Works

This paper has introduced the satellite eavesdropping approach, where a spacecraft eavesdrops on an LEO satellite. Specifically, we assumed an LEO satellite communicating with a HAPS node in the presence of an attacker spacecraft located very close to the LEO satellite. The unified expressions of SOP and ASC were derived in closed-form assuming EW fading. The expressions obtained were validated with MC simulations. In addition, the simulation results showed that satellite-to-HAPS downlink communication is more secure. It was also shown that increasing the leaked beam collected by the eavesdropping spacecraft deteriorated the secrecy performance. We observed that turbulence-induced fading highly affected the secrecy performance.

The future work directions can be summarized as follows: PLS techniques against wireless eavesdroppers as wiretap coding will be studied while exploiting the channel characteristics along with the transceiver architecture in order to favor the data transmission between legitimate users. Finally, optimization of the ST by adjusting the target secrecy rate and the power allocation ratio will be carried out.

REFERENCES

[1] G. Karabulut 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.

[2] M. S. Alam, G. K. Kurt, H. Yanikomeroglu, P. Zhu, and N. Dáo, "High altitude platform station based super macro base station constellations," *IEEE Commun. Mag.*, vol. 7, no. 1, pp. 103–109, Jan. 2021.

[3] 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.

[4] S. C. Arum, D. Grace, and P. D. Mitchell, "A review of wireless communication using high-altitude platforms for extended coverage and capacity," *Comput. Commun.*, vol. 157, pp. 232–256, 2020.

[5] 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.

[6] S. R. 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.

[7] Y. Shi, Y. Gao, and Y. Xia, "Secrecy performance analysis in internet of satellites: Physical layer security perspective," in *Proc. Int. Conf. Commun. China*, 2020, pp. 1185–1189.

[8] R. Boluda-Ruiz and K. Qaraqe, "Effect of misalignment error on secrecy outage capacity of FSO communication links," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2019, pp. 1–7.

[9] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of FSO communications over Málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, pp. 1–17, Dec. 2020.

[10] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, Apr. 2015.

[11] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over Málaga turbulence channels," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 274–277, Apr. 2017.

[12] P. V. Trinh, A. Carrasco-Casado, A. T. Pham, and M. Toyoshima, "Secrecy analysis of FSO systems considering misalignments and eavesdropper's location," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7810–7823, Dec. 2020.

[13] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Maximum secrecy throughput of MIMOME FSO communications with outage constraints," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 3487–3497, May 2018.

[14] J. Zhu, Y. Chen, and M. Sasaki, "Average secrecy capacity of free-space optical communication systems with on-off keying modulation and threshold detection," in *Proc. IEEE Int. Symp. Inf. Theory Appl.*, 2016, pp. 616–620.

[15] P. Norris, *Spies in the Sky: Surveillance Satellites in War and Peace*. Berlin, Germany: Springer, 2007.

[16] O. Ben Yahia *et al.*, "Physical layer security framework for optical non-terrestrial networks," in *Proc. Int. Conf. Telecommun.*, 2021, pp. 162–166.

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

[18] E. Erdogan, I. Altunbas, G. K. Kurt, M. Bellemare, G. Lamontagne, and H. Yanikomeroglu, "Site diversity in downlink optical satellite networks through ground station selection," *IEEE Access*, vol. 9, pp. 31179–31190, 2021.

[19] E. Erdogan, N. Kabaoglu, I. Altunbas, and H. Yanikomeroglu, "On the error probability of cognitive RF-FSO relay networks over Rayleigh/EW fading channels with primary-secondary interference," *IEEE Photon. J.*, vol. 12, no. 1, pp. 1–13, Feb. 2020.

[20] O. Ben Yahia, E. Erdogan, and G. Karabulut Kurt, "HAPS-assisted hybrid RF-FSO multicast communications: Error and outage analysis," 2021, *arXiv:2109.10131*.

[21] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[22] N. A. Sarker *et al.*, "Secrecy performance analysis of mixed hyper-gamma and gamma-gamma cooperative relaying system," *IEEE Access*, vol. 8, pp. 131273–131285, 2020.

[23] The Wolfram functions site. Accessed: Nov. 2, 2021. [Online]. Available: http://www.wolfram.com

[24] O. Ben Yahia, E. Erdogan, and G. Karabulut Kurt, "On the use of HAPS to increase secrecy performance in satellite networks," in *Proc. IEEE Int. Conf. Commun. Workshops*, 2021, pp. 1–6.

[25] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Norwell, MA, USA: Academic Press, 2014.

[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.

[27] D. R. Pattanayak, V. K. Dwivedi, V. Karwal, I. S. Ansari, H. Lei, and M.-S. Alouini, "On the physical layer security of a decode and forward based mixed FSO/RF co-operative system," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 1031–1035, Jul. 2020.