ITU/JWCC

Improving Secrecy Performance in Optical HAPS Communications Through Site Selection Under Harsh Weather Conditions

Eylem Erdogan[1], **Evla Safahan Ahrazoglu**[2], **Emre Berker Bakirci**[2], **and Ibrahim Altunbas**[2]

[1] Department of Electrical and Electronics Engineering, Izmir Institute of Technology, Izmir, 35430, Turkey
[2] Department of Electronics and Communication Engineering, Istanbul Technical University, Istanbul, 34469, Turkey

Abstract: The physical layer security of non-terrestrial networks (NTNs) has recently garnered increasing attention from both academia and industry as the information can be intercepted in aerial transmissions, especially when an illegitimate user positions itself near the transmitter or receiver. To address this vulnerability, we investigate the secrecy performance of a high altitude platform station (HAPS) system using optical communications in the presence of an aircraft eavesdropper. Specifically, we assess the secrecy-reliability trade-off by considering both outage and interception probability, and explore the secrecy outage probability. In the proposed setup, we evaluate a practical scenario in which the HAPS communicates with multiple ground stations located at different altitudes, examining the system's physical layer security performance for different types of attenuators including fog, clouds and air pollution. The findings indicate that weather conditions significantly affect the secrecy performance of optical HAPS communications. However, placing ground stations at higher altitudes or selection among multiple ground stations can improve the overall security performance of the system.

Keywords: HAPS systems, optical communication, physical layer security.

Zorlu Hava Koşulları Altında Yer İstasyonu Seçimi Yoluyla Optik HAPS İletişiminde Gizlilik Başarımının Arttırılması

Özet: Son zamanlarda, havasal iletimlerde bilginin ele geçirilebilmesi nedeniyle, karasal olmayan ağların (non-terrestrial networks, NTNs) fiziksel katman güvenliği hem akademide hem de endüstride artan bir ilgiyle karşılanmaktadır; özellikle de yetkisiz bir kullanıcının vericiye veya alıcıya yakın bir konumda bulunması durumunda güvenlik riskleri artmaktadır. Olası güvenlik açıklarını ele almak amacıyla, bu çalışmada optik haberleşme kullanan bir yüksek irtifa platform istasyonu (high altitude platform station, HAPS) sisteminin gizlilik performansı, bir gizli dinleyicinin varlığı altında incelenmiştir. Özellikle, kesinti ve ele geçirilme olasılıklarını dikkate alarak önerilen sistemin gizlilik-güvenilirlik dengesi değerlendirilmiş ve gizlilik kesinti olasılığı hesaplanmıştır. Önerilen senaryoda, HAPS'ın farklı yüksekliklerde konumlanmış birden fazla yer istasyonu ile iletişim kurduğu pratik bir durumu ele alarak, sistemde sis, bulutlar ve hava kirliliği gibi farklı zayıflatıcı etmenlerin etkisi incelenmiştir. Sonuçlar, hava koşullarının optik HAPS iletişimlerinin gizlilik performansını önemli ölçüde etkilediğini göstermektedir. Ancak, yer istasyonlarının daha yüksek irtifalarda konumlandırılması veya birden fazla yer istasyonu arasından seçim yapılması sistemin genel güvenlik performansını arttırabilmektedir.

Anahtar Kelimeler: HAPS sistemleri, optik haberleşme, fiziksel katman güvenlik.

RESEARCH PAPER

Corresponding Author: Eylem Erdogan, eylemerdogan@iyte.edu.tr

Reference: E. Erdogan, E. S. Ahrazoglu, E. B. Bakirci, and I. Altunbas, (2025), "Improving Secrecy Performance in Optical HAPS Communications Through Site Selection Under Harsh Weather Conditions," *ITU-Journ. Wireless Comm. Cyber.*, 2, (1) 1–10.

Submission Date: Nov, 26, 2024
Acceptance Date: Mar, 2, 2025
Online Publishing: Mar, 28, 2025

1 INTRODUCTION

Due to the foreseen increase in requested data rates from the users, different techniques aiming to convey more information to the users are among the key topics of interest for researchers today. Free space optics (FSO) offers a promising solution to the growing demand for higher data rates, leveraging the broader bandwidth available at optical frequencies to transmit large volumes of data. One distinctive feature of optical signals is their highly directional beams, which restricts their use to line-of-sight (LOS) scenarios, unlike traditional radio frequency (RF) communication where a LOS link is not always required. However, this signal characteristic also addresses another critical issue: data privacy [1]. Unlike RF signals, where electromagnetic wave propagation raises security concerns, an eavesdropper in FSO systems must be positioned close to the LOS link to be able to listen the legitimate user, thereby enhancing the security of transmitted data [2].

An alternative approach to address user privacy concerns can be established by using physical layer security (PLS) techniques, which provide information-theoretic security by exploiting the inherent randomness in wireless channels, such as noise and fading characteristics. PLS techniques ensure secure communication as long as the legitimate user's channel quality surpasses those of potential eavesdroppers [3]. Compared to the traditional cryptographic methods, PLS techniques offer greater computational efficiency and ease of implementation, making them a topic of increasing interest among both researchers and industry professionals in the recent years [4].

Aiming to satisfy both high data rate and security requirements, various scenarios that utilize FSO technique have been analyzed in the literature. [1] and [5] derive the secrecy performance of a single hop FSO link under different turbulence channels. Reference [6] extends the single hop analysis to multiple scenarios for different eavesdropper locations, and [2] focuses on secrecy performance under different eavesdropper locations. Moreover, [7] and [8] add an RF link to the single hop scenarios, with and without an additional RF eavesdropper, respectively. Finally, [9] and [10] analyze multi hop hybrid FSO/RF scenarios with maximum ratio combining (MRC) and selection combining (SC) diversity reception techniques respectively.

Another promising approach for providing stable and high-rate data transmission to targeted users is the implementation of vertical networks, which can be realized through unmanned aerial vehicles (UAVs), high-altitude platform stations (HAPS), or low Earth orbit (LEO) satellites. In HAPS enabled communications, stronger and less disrupted LOS communication can be provided to a large number of user, with enhanced data rates, and reliable communication performance [11]. However, as these networks serve a large number of users, higher privacy demands arise. Consequently, the need for comprehensive research and detailed analysis of vertical network scenarios becomes essential to address these growing privacy concerns effectively.

In the recent years, secrecy performance of vertical networks with PLS techniques have been investigated in the literature. Among them, [12] analyzes a downlink satellite communication scenario where the receiver and the eavesdropper are equipped with multiple antennas. Reference [13] explores the impact of satellite orbits on secrecy performance, while [3] examines a satellite communication scenario that incorporates channel estimation errors and considers the presence of multiple receivers along with multiple eavesdroppers. Moreover, [14] analyzes the secrecy performance of a scenario in which multiple relays are fed from a satellite and paired with multiple users, and [15] includes power optimization and trajectories of UAV's to improve secrecy performance. Finally, [16] focuses on the secrecy performance of a multiple UAV relay assisted system setup. In addition to the aforementioned studies, numerous papers in the literature have explored the integration of the high data rates provided by FSO techniques with the extensive coverage capabilities of vertical networks to enhance secrecy. For instance, [17] examines the secrecy performance of a single-hop FSO link between a LEO satellite and a HAPS system. Similarly, [18] explores various scenarios in non-terrestrial networks, including LEO satellite-to-HAPS, HAPS-to-HAPS, and HAPS-to-ground links. Furthermore, [19] introduces a hybrid FSO/RF link in addition to the FSO link between a LEO satellite and a HAPS, enhancing communication robustness.

In addition to the above-mentioned studies, several secrecy analyses have been conducted in the literature, combining both the high data rate output of FSO techniques and the robustness of vertical networks. For instance, [17] examines the secrecy performance of a single-hop FSO link between a LEO satellite and a HAPS. Similarly, [18] explores various scenarios in non-terrestrial networks, including LEO satellite-to-HAPS, HAPS-to-HAPS, and HAPS-to-ground links. Furthermore, [19] introduces a hybrid FSO/RF link in addition to the FSO link between a LEO satellite and a HAPS, enhancing communication robustness.

Building upon the principles of FSO communication and PLS, this study presents a comprehensive analysis of physical layer security in HAPS systems utilizing optical communication. Given the growing demand for secure and high-rate communication in non-terrestrial networks, particularly with the unique characteristics of FSO such as narrow beamwidth and high directivity, our research focuses on evaluating the secrecy performance of HAPS-based optical communication links. The contributions of this paper can be summarized as follows:

- By integrating the strengths of optical transmission with the security benefits offered by PLS techniques, we provide a thorough investigation into how these systems can ensure secure communication against potential eavesdropping threats. To do so, we consider different site deployment scenarios in the presence of various attenuators, including fog, clouds, and air pollution.

- The analysis is crucial as HAPS systems, positioned in the stratosphere, present distinct challenges and opportunities in terms of maintaining high-quality, secure communication links over vast areas. To establish a practical scenario, we consider an aerial eavesdropper positioned close to the HAPS node, trying to intercept optical communication.
- In this study, we analyze the impact of various weather conditions and deployment scenarios on system performance, with a primary focus on the secrecy outage probability. Furthermore, we examine the security-reliability trade-off by jointly considering outage probability and intercept probability. By evaluating these factors in the proposed scenario, we aim to provide a deeper understanding of how environmental conditions and site configurations influence both the security and reliability of the system.

The paper is organized as follows. In Section 2.1, a general system model is described, followed by explanations about atmospheric attenuation and turbulence-induced fading channel in Section 2.2. Section 2.3 focuses on clarifying different scenarios that will be used throughout the paper. Section 3 focuses on statistical properties of SNR and analytical expressions about secrecy performance of the proposed system. Simulation results are talked upon in Section 4, and the results are summarized in Section 5.

2 SYSTEM AND CHANNEL MODEL

2.1 System Model

In this study, we introduce a scenario for an eavesdropping attack on the communication link between a HAPS system and a ground station. Specifically, we analyze the case where HAPS A is communicating with the best site B_k^*, among possible sites B_k, $k \in \{1,2,...,N\}$ in the footprint of A. This capability allows A to enhance the secrecy performance of the communication by strategically choosing the optimal site from a range of possible candidates [20]. Meanwhile, the aircraft eavesdropper E, positioned in close proximity to A, is actively attempting to intercept and gather information transmitted through the optical beam as illustrated in Fig. 1. Positioning itself above the troposphere enhances E's eavesdropping performance by mitigating the impacts of weather-dependent effects. However, despite this advantage, intercepting information in optical communication remains challenging, as any eavesdropper in close proximity to A must block the LOS communication between A and B_k to successfully gather the data. Alternatively, E could function as a passive optical beam splitter, capturing a small fraction r_E of the laser beam's irradiance, while allowing the remainder r_{B_k} to be transmitted to B_k satisfying $r_{B_k} + r_E = 1$ [1]. For the proposed structure, the received signals at B_k and E can be written as

$$y_{B_k} = \sqrt{r_{B_k} P_A} I_{B_k} g_{B_k} x + n_{B_k}, \tag{1}$$

and

$$y_E = \sqrt{r_E P_A} I_E g_E x + n_E, \tag{2}$$

where P_A is the transmit power of A, n_{B_k} stands for the additive white Gaussian noise (AWGN) with one-sided noise power N_0, I_{B_k} is turbulence induced fading channel coefficient, and g_{B_k} denotes the atmospheric attenuation between A and B_k respectively. Moreover, I_E and g_E are the turbulence induced fading coefficient and attenuation between A and E, and n_E is the AWGN noise at passive eavesdropper with one-sided noise power N_0. Accordingly, the instantaneous SNRs at B_k and E can be written as

$$\gamma_j = \frac{r_j P_A}{N_0} I_j^2 g_j^2 = \overline{\gamma}_j I_j^2, \tag{3}$$

where $j \in \{B_k, E\}$, and $\overline{\gamma}_j = \frac{r_j P_A}{N_0} g_j^2$ is the average SNR with $E[I_j^2] = 1$.

2.2 Channel Model

The optical signal's quality is influenced by various atmospheric factors, such as weather conditions, turbulence, and random fluctuations as it travels through the atmosphere. Key factors include atmospheric conditions like cloud formations, fog, dust, rain, and snow, which cause scattering, absorption, and attenuation of the signal due to changes in the refractive index along the transmission path. In this section, we briefly summarize these limiting effects.

2.2.1 Atmospheric attenuation

In optical communication systems, atmospheric attenuation is caused by scattering and absorption, both of which are affected by atmospheric particles and weather phenomena, especially fog and clouds.[1]. Mathematically, atmospheric attenuation is expressed as $g_{B_k} = g_{B_k}^{\text{mie}} g_{B_k}^{\text{geo}}$, where $g_{B_k}^{\text{mie}}$ and $g_{B_k}^{\text{geo}}$ represent the attenuation due to Mie scattering and geometrical scattering, respectively. Mie scattering occurs when the wavelength of operation is similar to the size of the particles in the transmission medium, and its behavior can be described as [21]

[1] As a HAPS eavesdropper, E remains impervious to weather-dependent effects. Consequently, the analysis presented herein remains applicable to the communication between A and B_k.

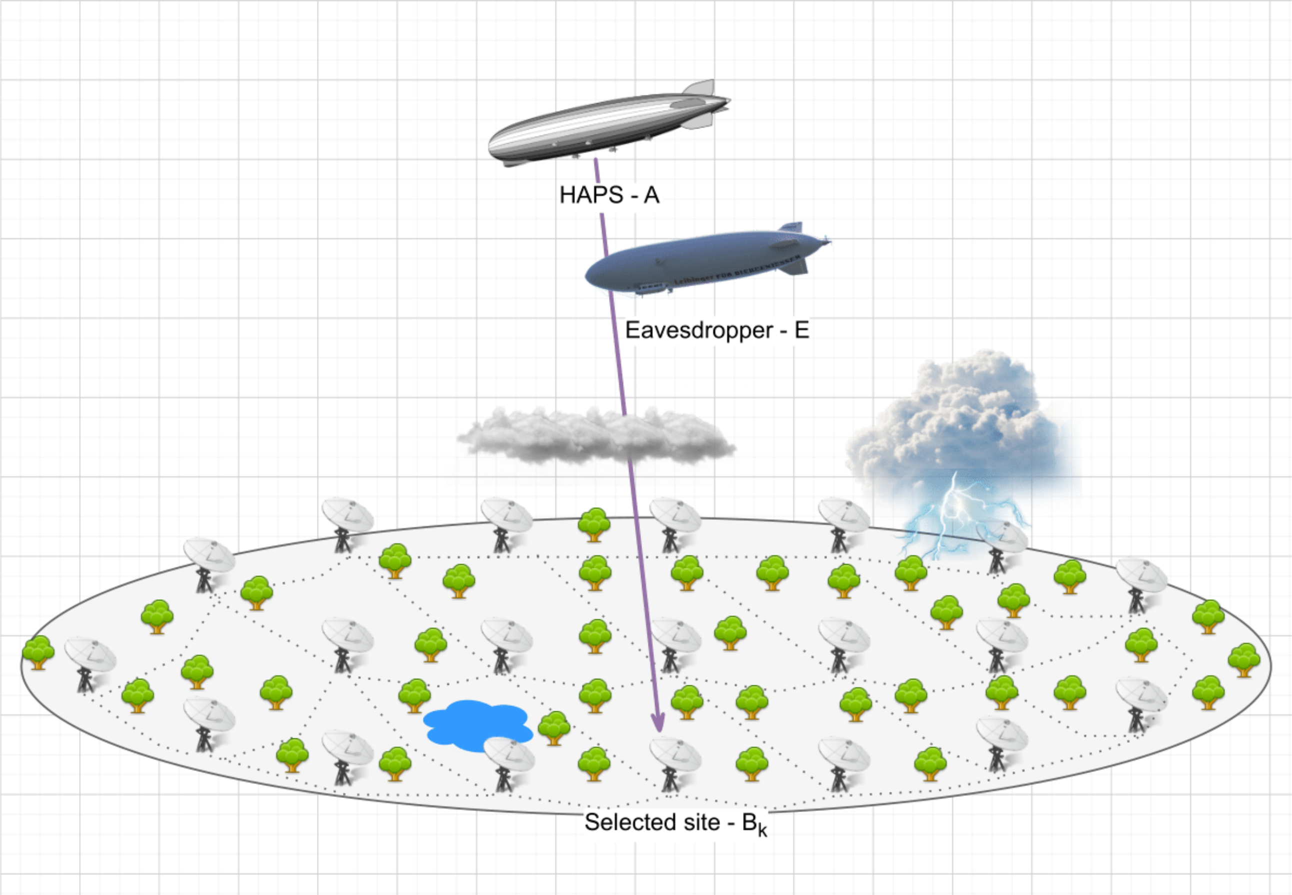

Fig. 1 Illustration of HAPS to ground station communication with a HAPS eavesdropper.

$$g_{B_k}^{\text{mie}} = \exp\left(-\frac{\rho'}{\sin(\theta_{B_k})}\right), \tag{4}$$

where θ_{B_k} is the elevation angle between A and B_k-th site. Here, ρ' denotes the extinction ratio and it is defined as [21]

$$\rho' = a' h_{B_k}^3 + b' h_{B_k}^2 + c' h_{B_k} + d', \tag{5}$$

where h_{B_k} is the height of the selected site above mean sea level. a', b', c', and d' depend on the signal wavelength λ through the following equations

$$\begin{aligned} a' &= -0.000545\lambda^2 + 0.002\lambda - 0.0038, \\ b' &= 0.00628\lambda^2 - 0.0232\lambda + 0.0439, \\ c' &= -0.028\lambda^2 + 0.101\lambda - 0.18, \\ d' &= -0.228\lambda^3 + 0.922\lambda^2 - 1.26\lambda + 0.719. \end{aligned} \tag{6}$$

Geometrical scattering, on the other hand, is associated with the optical visibility range, which is influenced by cloud/fog formations and atmospheric pollution. Based on the Kim's model, the attenuation caused by geometrical scattering can be expressed as [22]

$$g_{B_k}^{\text{geo}} = \exp(-\varphi_{B_k} D_{B_k}^{\text{geo}}), \tag{7}$$

where $D_{B_k}^{\text{geo}}$ is the distance of the fraction of the link between A to B_k that experiences geometrical scattering, and φ_{B_k} denotes the attenuation coefficient, defined as [22]

$$\varphi_{B_k} = \frac{3.91}{V_{B_k}} \left(\frac{\lambda}{550}\right)^{-\psi_{B_k}}, \tag{8}$$

where ψ_{B_k} and V_{B_k} are the particle size coefficient and optical visibility, and ψ_{B_k} is determined by the Kim's model as [23]

$$\psi_{B_k} = \begin{cases} 1.6 & V_{B_k} > 50 \\ 1.3 & 6 < V_{B_k} < 50 \\ 0.16V_{B_k} + 0.34 & 1 < V_{B_k} < 6 \\ V_{B_k} - 0.5 & 0.5 < V_{B_k} < 1 \\ 0 & V_{B_k} < 0.5. \end{cases} \tag{9}$$

Herein, V_{B_k} is defined as [23]

$$V_{B_k} = \frac{1.002}{(\mathscr{W}_{B_k}\mathscr{C}_{B_k})^{0.6473}} \text{ [km]}, \tag{10}$$

where $\mathscr{W}_{B_k}$ and $\mathscr{C}_{B_k}$ denote liquid water content and cloud number concentration. The values of $\mathscr{W}_{B_k}$, $\mathscr{C}_{B_k}$, and V_{B_k}, under $\lambda = 1550nm$, for various cloud formations are presented in Table 1. Moreover, V_{B_k} and φ_{B_k} values for fog formations and different atmospheric pollution levels are provided in Table 2 and 3, respectively.

Table 1 Geometrical scattering parameters for different cloud formations at $\lambda = 1550$ nm [23]

Cloud formation	$\mathscr{W}_{B_k}$ [cm^{-3}]	$\mathscr{C}_{B_k}$ [g/m^{-3}]	V_{B_k} [km]
Cumulus	250	1.0	0.028
Stratus	250	0.29	0.0626
Stratocumulus	250	0.15	0.0959
Altostratus	400	0.41	0.0369
Nimbostratus	200	0.65	0.0429
Cirrus	0.025	0.06405	64.66
Thin cirrus	0.5	3.128×10^{-4}	290.69

Table 2 Geometrical scattering parameters for different fog formations [24]

Fog formation	V_{B_k} [km]	φ_{B_k} [dB/km]
Dense	0.05	339.62
Thick	0.2	84.9
Moderate	0.5	33.96
Light	0.77	16.67
Thin	1.9	4.59

Table 3 Geometrical scattering parameters for different atmospheric pollution levels [25]

Atmospheric pollution	V_{B_k} [km]	φ_{B_k} [dB/km]
Extremely polluted atm.	1 (low)	16.98
Normal atm.	10 (mod)	0.442
Non-polluted atm. (clear)	145 (high)	0.022

2.2.2 Turbulence-induced fading

Atmospheric temperature fluctuations give rise to turbulent eddies with randomly varying refractive indices. As these eddies function like dynamic optical lenses, they introduce random variations in the amplitude of the transmitted signal, a phenomenon termed turbulence-induced fading. This fading can be effectively modeled using the exponentiated Weibull distribution (EW) [26], where the probability density function (PDF) and cumulative distribution function (CDF) characterize the statistical behavior of signal fluctuations as

$$f_I(I) = \frac{\alpha\beta}{\eta}\left(\frac{I}{\eta}\right)^{\beta-1} \exp\left[-\left(\frac{I}{\eta}\right)^{\beta}\right]\left(1 - \exp\left[-\left(\frac{I}{\eta}\right)^{\beta}\right]\right)^{\alpha-1}, \tag{11}$$

and

$$F_I(I) = \left(1 - \exp\left[-\left(\frac{I}{\eta}\right)^{\beta}\right]\right)^{\alpha}, \tag{12}$$

respectively. Here, α and β are the distribution parameters, and η is the scale parameter. The parameters can be expressed as [27]

$$\begin{aligned} \alpha &= \frac{7.22\sigma_I^{2/3}}{\Gamma\left(2.487\sigma_I^{2/6} - 0.104\right)}, \\ \beta &= 1.012\left(\alpha\sigma_I^2\right)^{-13/25} + 0.142, \\ \eta &= \frac{1}{\alpha\Gamma(1+1/\beta)\,g_1(\alpha,\beta)}, \end{aligned} \tag{13}$$

where $g_1(\alpha,\beta)$ is defined as

$$g_1(\alpha,\beta) \triangleq \sum_{k=0}^{\infty} \frac{(-1)^k\Gamma(\alpha)}{k!(k+1)^{1+1/\beta}\Gamma(\alpha-k)}. \tag{14}$$

In this formulation, the fluctuation level can be obtained by using the scintillation index σ_I^2, which is determined by the Rytov variance σ_R^2 as [28]

$$\sigma_I^2 = \exp\left[\frac{0.49\sigma_R^2}{(1+1.11\sigma_R^{12/5})^{7/6}} + \frac{0.51\sigma_R^2}{(1+0.69\sigma_R^{12/5})^{5/6}}\right] - 1, \tag{15}$$

and the Rytov variance σ_R^2 is related with the physical parameters, including transmitter and receiver altitudes, wind speed, wave number and the zenith angle. Further details about the calculation of σ_R^2 can be found in [28].

2.3 Site Deployment Model

In the forthcoming generation of optical wireless communication systems, multiple ground stations may be strategically positioned at varying altitudes above mean sea level to optimize coverage and enhance performance. Specifically, deploying multiple stations within NTNs offers a viable solution for mitigating signal attenuation caused by adverse weather conditions. With practical deployment in mind, we propose three distinct deployment strategies in this work.

In the scenario of ground level deployment, we consider that all sites available for communication are situated at ground level, precisely $h_0 = 0$ km above the surface and $h_E = 0.01$ km above mean sea level, where the wind speed is 2.8 m/s, and $\lambda = 1550$ nm. In the configuration of mid-level deployment, we assume the ground stations are positioned at mid-altitudes, such as on hills, low mountainous regions, or foothills, to minimize signal attenuation. The altitudes are set to $h_0 = 0.5$ km and $h_E = 0.7$ km. As a result, the wind speed experiences a slight increase to 5.1 m/s, with an operational wavelength of $\lambda = 1550$ nm. In the setup of high-level deployment, the ground stations are located at very high altitudes, like high plateau, or mountains. As a result, h_0 and h_E are taken as $h_0 = 2$ km and $h_E = 2.2$ km, and the wind speed increases up to 10.0 m/s, with the same operational wavelength as given above.

3 SECRECY PERFORMANCE ANALYSIS

In this section, we first present the statistical properties of SNR. Thereafter, we analyze the proposed system in terms of secrecy outage probability (SOP) and provide a security-reliability trade-off.

3.1 Statistical Properties of SNR

The proposed site selection method relies on the maximization of SNR. Mathematically, the best site is selected as

$$k^* = \arg \max_{1 \leq k \leq N} \left[\gamma_{B_k}\right], \tag{16}$$

and similarly, the end-to-end SNR at the legitimate link can be written as

$$\gamma_B = \max_{1 \leq k \leq N} [\gamma_{B_k}]. \tag{17}$$

Assuming independent identically distributed Exponentiated Weibull random variables in each link, with the aid of (12) and (17) CDF of the overall SNR can be expressed as

$$F_{\gamma_B}(\gamma_B) = \prod_{k=1}^{N} \left(1 - \exp\left[-\left(\frac{\gamma_B}{\left(\eta_{B_k} g_{B_k}\right)^2 \bar{\gamma}_{B_k}}\right)^{\beta_k/2}\right]\right)^{\alpha_k}. \tag{18}$$

3.2 Secrecy Outage Probability

In the physical layer security, SOP stands as one of the most extensively employed metrics for evaluating secrecy performance in academic literature. Within the context of wireless communications, HAPS A must ensure that the information is transmitted at a fixed secrecy rate, denoted by R_s. For secure communication to be maintained, this secrecy rate is required to be less than the secrecy capacity C_s, meaning that the condition $C_s > R_s$ must hold true to prevent a breach in secrecy [29]. Mathematically, SOP can be defined as

$$P_{\text{SO}} = \Pr[C_s < R_s], \tag{19}$$

where $R_s = \log_2 \gamma_{th}$, and C_s can be written as

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

As we assume a turbulence-free communication model between B and E, due their close proximity, the SNR at E, denoted as γ_E, can be represented by its average value $\bar{\gamma}_E$, given by $\gamma_E = \bar{\gamma}_E = \frac{r_E P_A}{N_0}$ [1]. Therefore, by invoking (20) into (19), P_{SO} can be written as

$$P_{\text{SO}} = \Pr[\gamma_B < \gamma_{th}(1 + \bar{\gamma}_E) - 1], \tag{21}$$

and with the aid of (21), and (18), P_{SO} can be expressed as

$$P_{\text{SO}} = \prod_{k=1}^{N} \left(1 - \exp\left[-\left(\frac{\gamma_{th}(1 + \bar{\gamma}_E) - 1}{\left(\eta_{B_k} g_{B_k}\right)^2 \bar{\gamma}_{B_k}}\right)^{\beta_k/2}\right]\right)^{\alpha_k}. \tag{22}$$

3.3 Security-Reliability Trade-off

The security-reliability trade-off (SRT) is characterized by the balance between the intercept probability (IP) and the outage probability (OP) in communication systems [30]. IP refers to the probability that E successfully intercepts and decodes the transmitted signal. This happens when the E's SNR exceeds a certain threshold, allowing it to capture the data. On the contrary, OP measures the probability that the signal quality, typically quantified by SNR of the legitimate link, falls below a certain threshold γ_{th}. By taking IP and OP into consideration, the SRT can be expressed as [30]

$$P_{\text{SRT}} = \Pr[\gamma_B \leqslant \gamma_E, \gamma_E > \gamma_{th}]. \tag{23}$$

Please note that IP and OP are statistically independent. Therefore the above expression can be written as $P_{\text{SRT}} = \Pr[\gamma_B \leqslant \gamma_E]\Pr[\gamma_E > \gamma_{th}]$. Therefore, P_{SRT} can be expressed

$$\begin{aligned} P_{\text{SRT}} &= \Pr[\gamma_B \leqslant \gamma_E]\Pr[\gamma_E > \gamma_{th}] \\ &= \Pr[\gamma_E > \gamma_{th}] \prod_{k=1}^{N} \left(1 - \exp\left[-\left(\frac{\bar{\gamma}_E}{\left(\eta_{B_k} g_{B_k}\right)^2 \bar{\gamma}_{B_k}}\right)^{\beta_k/2}\right]\right)^{\alpha_k}. \end{aligned} \tag{24}$$

Morever, SRT can be asymptotically evaluated by using the high SNR Taylor expansion of $\exp(x) \cong 1 - x$ as

$$P_{\text{SRT}}^{\infty} = \Pr[\gamma_E > \gamma_{th}] \prod_{k=1}^{N} \left(\frac{\bar{\gamma}_E}{\left(\eta_{B_k} g_{B_k}\right)^2 \bar{\gamma}_{B_k}}\right)^{\alpha_k \beta_k/2}. \tag{25}$$

4 NUMERICAL RESULTS

In this section, the SOP and SRT performances of the proposed system are illustrated, and theoretical findings are validated by Monte-Carlo simulations. It is assumed that HAPS A is employed at an altitude of 30 km as recommended in [31] and that the eavesdropper E is located at very close proximity of HAPS A. Due to close distance between A and E, we assume that $\Pr[\gamma_E > \gamma_{th}] = 0.9$. The zenith angles between the A and all possible sites are assumed to be $\zeta = 10^\circ$. Three different site deployment scenarios are considered as described in Section 2.3, and the fading parameters are found as $\alpha = 3.209$, $\beta = 2.505$, $\eta = 0.81$ for the ground level deployment, $\alpha = 3.113$, $\beta = 2.657$, $\eta = 0.827$ for the mid-level deployment, and $\alpha = 3.135$, $\beta = 2.621$, $\eta = 0.823$ for the high-level deployment. The distances $D_{B_k}^{\text{geo}}$ are calculated through measurement results in [32]. Additionally, the fixed secrecy rate is taken as $R_s = 1$ bit/s, and the fraction of the power received by the eavesdropper is set to $r_E = 0.2$. Also, the received SNR at the eavesdropper is assumed as $\bar{\gamma}_E = 5$ dB.

In Fig. 2, the SOP performance of the system is shown for the ground level deployment scenario in the presence of thin cirrus cloud formation with $D_{B_k}^{\text{geo}} = 0.1$ km for different number of sites. It can be seen here that the theoretical results are perfectly matched with the simulations. Moreover, it is inferred from the figure that the slopes of the curves increase with the increasing number of sites. This stems from larger diversity order offered by higher number of sites. Hence, it can be deduced that enhanced security can be achieved by deploying higher number of sites.

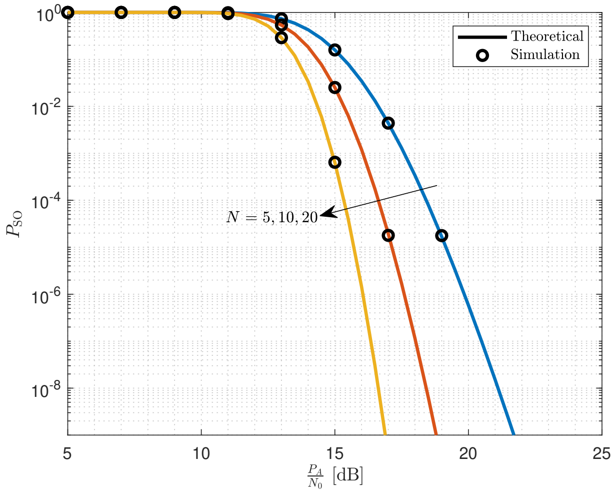

Fig. 2 SOP performance of the system under thin cirrus cloud formation for the ground level deployment and $N = 5, 10, 20$.

The SOP curves for $N = 10$ sites are illustrated in Fig. 3 for different deployment scenarios in the presence of thin cirrus cloud formation with $D_{B_k}^{\text{geo}} = 0.1$ km. It can be observed from the figure that the system performance is enhanced from ground level to mid-level deployment and from mid-level to high-level deployment. Therefore, it can be said that utilizing higher altitudes for sites improves the system performance. Notice here that the slopes of the curves are almost the same, and the system performance is improved in terms of power gain. This can be attributed to lower loss levels owing to high-level deployment and shorter link distance.

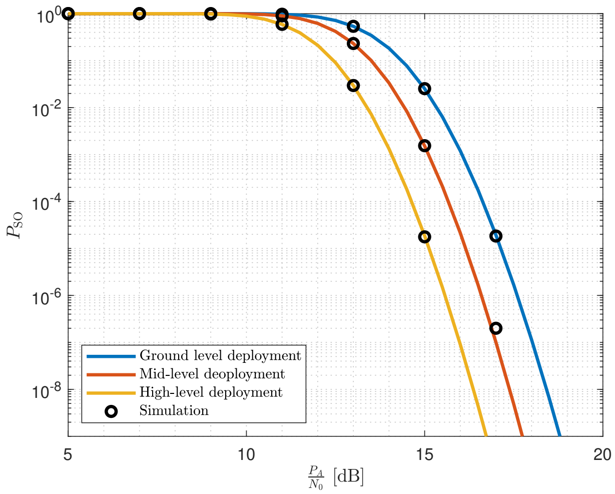

Fig. 3 SOP performance of the system under thin cirrus cloud formation for different deployment scenarios and $N = 10$.

In Fig. 4, the SOP performance is presented with respect to r_E for different deployment scenarios, fixed $\frac{P_A}{N_0} = 15$ dB, and $N = 10$ number of sites. Here, thin cirrus cloud formation is considered with $D_{B_k}^{\text{geo}} = 0.1$ km. It can be inferred from the figure that deploying sites at higher altitudes significantly improves the system performance for lower values of r_E. However, for higher values of r_E, SOP dramatically increase. This can be explained by the fact that the eavesdropper receives very large fraction of the transmitter power and the legitimate sites receive very small fraction of the power. Thus, secure communication becomes infeasible for high values of r_E.

In Fig. 5, the SOP curves are illustrated for $N = 10$ number of sites with mid-level deployment under different atmospheric conditions. Here, thin cirrus cloud formation with $D_{B_k}^{\text{geo}} = 0.1$ km, thin fog with $D_{B_k}^{\text{geo}} = 1.01$ km, and normal polluted atmosphere with $D_{B_k}^{\text{geo}} = 3.04$ km are considered to examine the effects of various visibility levels. It can be deduced from the figure that for a SOP of 10^{-9}, atmospheric pollution results in ~ 2.5 dB SNR loss in system performance, whereas thin fog formation introduces ~ 9 dB SNR loss. Hence, it can be concluded that the system performance significantly affected by the atmospheric conditions.

SRT performance of the proposed system is presented in Fig. 6 for $N = 5$ and mid-level deployment scenario under non-polluted, normal polluted, and extremely polluted

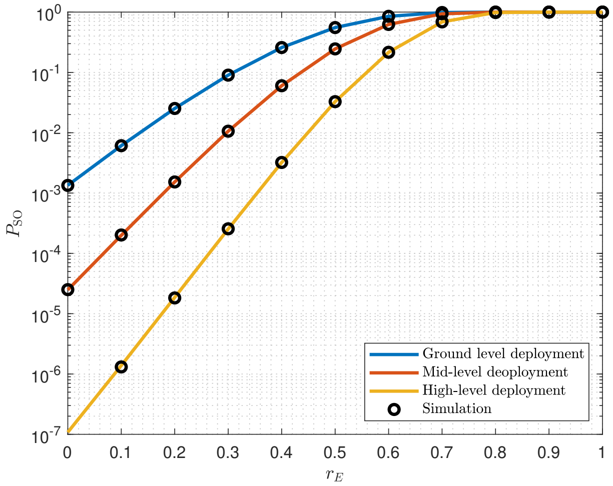

Fig. 4 SOP performance of the system with respect to r_E under thin cirrus cloud formation for $N = 10$ and $\frac{P_A}{N_0} = 15$ dB.

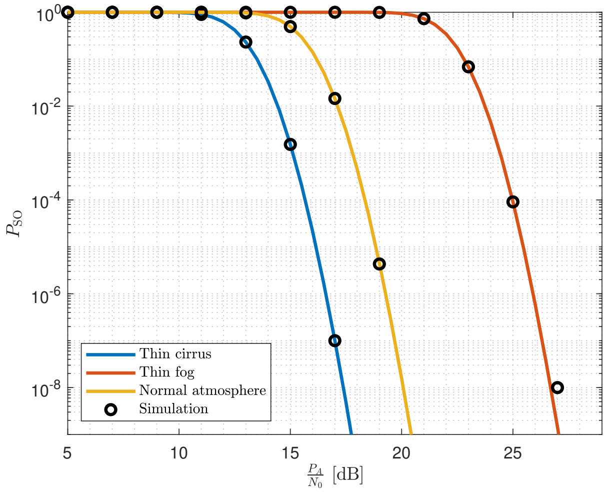

Fig. 5 SOP performance of the system under thin cirrus cloud formation, thin fog formation, normal polluted atmosphere for $N = 10$ and mid-level deployment.

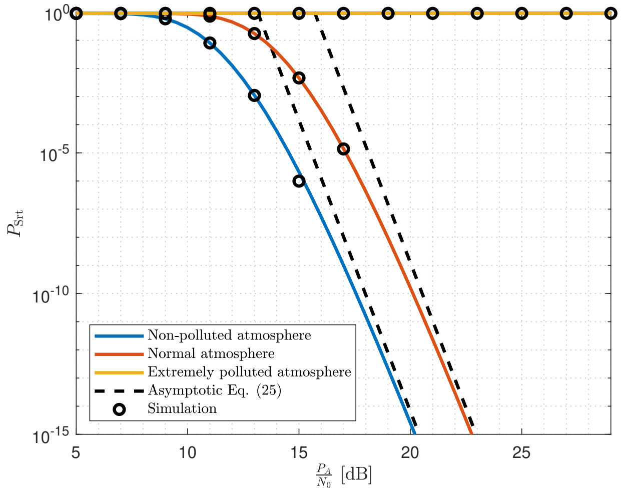

Fig. 6 Impact of pollution on SRT performance of the system for $N = 5$ and mid-level deployment scenario.

atmospheric conditions all with $D_{B_k}^{\mathrm{geo}} = 3.04$ km. It can be seen here that asymptotic curves perfectly depicts the system performance in high SNR region. Moreover, the figure reveals that different pollution regimes results in significant SNR loss in the system performance. Under extremely polluted atmosphere, reliable communication is not achievable with reasonable SNR values. Therefore it can be deduced that atmospheric pollution is critically important in SRT performance of the system.

In Fig. 7, SRT performance of the system is illustrated with respect to r_E for different deployment scenarios. Here, thin cirrus cloud formation with $D_{B_k}^{\mathrm{geo}} = 0.1$ km, $N = 10$ sites, and $\frac{P_A}{N_0} = 15$ dB are considered. It can be deduced from the figure that deploying legitimate sites at higher altitudes enhances the SRT performance of the system, similar to Fig. 4. Additionally, high values of r_E results in poor SRT performance, increasing up to probability of 1. This stems from the eavesdropper gathering most of the transmitted power, thus, secure communication between HAPS A and legitimate sites becomes infeasible.

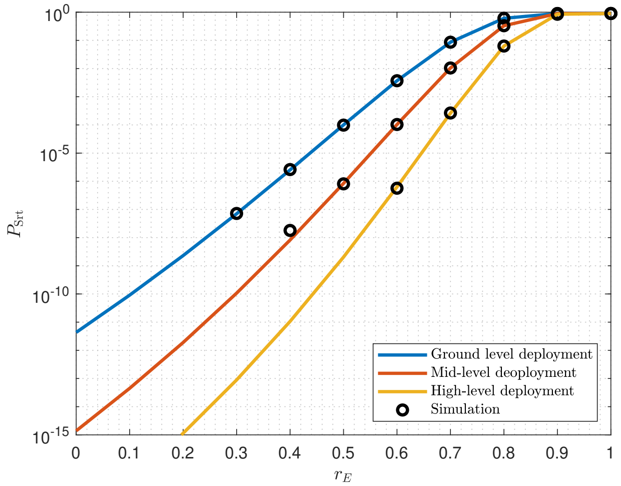

Fig. 7 SRT performance of the system with respect to r_E under thin cirrus cloud formation for $N = 10$ and $\frac{P_A}{N_0} = 15$ dB.

5 CONCLUSION

This study highlights the critical role that weather conditions play in the physical layer security of optical HAPS communications, particularly in the presence of an airborne eavesdropper. By evaluating the secrecy-reliability tradeoff through interception and outage probabilities, we have demonstrated that adverse weather conditions, such as fog, clouds, and air pollution, can severely degrade system performance. However, our results also show that strategically positioning ground stations at higher altitudes offers a viable solution to enhance overall secrecy. These insights provide valuable guidance for the design and deployment of secure non-terrestrial networks, emphasizing the need for careful consideration of environmental factors and system configuration in maintaining secure communications.

REFERENCES

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

[2] P. V. Trinh, A. Carrasco-Casado, A. T. Pham, and M. Toyoshima, “Secrecy analysis of FSO systems considering misalignments and eavesdropper’s location,” *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7810–7823, 2020.

[3] K. Guo, K. An, Y. Huang, and B. Zhang, “Physical layer security of multiuser satellite communication systems with channel estimation error and multiple eavesdroppers,” *IEEE Access*, vol. 7, pp. 96 253–96 262, 2019.

[4] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, “Physical layer security for ultra-reliable and low-latency communications,” *IEEE Wireless Communications*, vol. 26, no. 5, pp. 6–11, 2019.

[5] M. J. Saber and S. M. S. Sadough, “On secure free-space optical communications over Málaga turbulence channels,” *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 274–277, 2017.

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

[7] 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 Communications Letters*, vol. 9, no. 7, pp. 1031–1035, 2020.

[8] X. Pan, H. Ran, G. Pan, Y. Xie, and J. Zhang, “On secrecy analysis of DF based dual hop mixed RF-FSO systems,” *IEEE Access*, vol. 7, pp. 66 725–66 730, 2019.

[9] S. Althunibat, S. C. Tokgoz, S. Yarkan, S. L. Miller, and K. A. Qaraqe, “Physical layer security of dual-hop hybrid FSO-mmWave systems,” *IEEE Access*, vol. 11, pp. 58 209–58 227, 2023.

[10] D. R. Pattanayak, V. K. Dwivedi, V. Karwal, P. K. Yadav, and G. Singh, “Physical layer security analysis of multi-hop hybrid RF/FSO system in presence of multiple eavesdroppers,” *IEEE Photonics Journal*, vol. 14, no. 6, pp. 1–12, 2022.

[11] M. Alzenad, M. Z. Shakir, H. Yanikomeroglu, and M.-S. Alouini, “FSO-based vertical backhaul/fronthaul framework for 5G+ wireless networks,” *IEEE Communications Magazine*, vol. 56, no. 1, pp. 218–224, 2018.

[12] Y. Zhang, J. Ye, G. Pan, and M.-S. Alouini, “Secrecy outage analysis for satellite-terrestrial downlink transmissions,” *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1643–1647, 2020.

[13] Y. Xiao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, “Secure communication in non-geostationary orbit satellite systems: A physical layer security perspective,” *IEEE Access*, vol. 7, pp. 3371–3382, 2019.

[14] W. Cao, Y. Zou, Z. Yang, *et al.*, “Secrecy outage analysis of relay-user pairing for secure hybrid satellite-terrestrial networks,” *IEEE Transactions on Vehicular Technology*, vol. 71, no. 8, pp. 8906–8918, 2022.

[15] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, “UAV-enabled secure communications: Joint trajectory and transmit power optimization,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 4069–4073, 2019.

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

[17] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, “Optical satellite eavesdropping,” *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 10 126–10 131, 2022.

[18] E. Erdogan, O. B. Yahia, G. K. Kurt, and H. Yanikomeroglu, “Optical HAPS eavesdropping in vertical heterogeneous networks,” *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 208–216, 2023.

[19] V. Bankey, S. Sharma, S. R, and A. S. Madhukumar, “Physical layer security of HAPS-based space–air–ground-integrated network with hybrid FSO/RF communication,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 4, pp. 4680–4688, 2023.

[20] 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. 31 179–31 190, 2021.

[21] *Prediction Methods Required for the Design of Earth-Space Telecommunication Systems*, Rec. ITU-R P.1622, International Telecommunication Union, Geneva, Switzerland, 2003.

[22] I. I. Kim, B. McArthur, and E. J. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," vol. 4214, E. J. Korevaar, Ed., pp. 26–37, 2001.

[23] M. S. Awan, E. Leitgeb, B. Hillbrand, F. Nadeem, M. Khan, *et al.*, "Cloud attenuations for free-space optical links," in *2009 International Workshop on Satellite and Space Communications*, IEEE, 2009, pp. 274–278.

[24] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, "Haps selection for hybrid RF/FSO satellite networks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 2855–2867, 2022.

[25] S. Sabetghadam and F. Ahmadi-Givi, "Relationship of extinction coefficient, air pollution, and meteorological parameters in an urban area during 2007 to 2009," *Enviromental Science and Pollution Research*, vol. 21, pp. 538–547, 2014.

[26] R. Barrios and F. Dios, "Exponentiated weibull distribution family under aperture averaging for Gaussian beam waves," *Opt. Express*, vol. 20, no. 12, pp. 13 055–13 064, Jun. 2012.

[27] R. Barrios Porras, "Exponentiated Weibull fading channel model in free-space optical communications under atmospheric turbulence," Ph.D. dissertation, Dept. of Signal Theory and Commun., Univ. Politècnica de Catalunya, Barcelona, 2013.

[28] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media: Second Edition*, 2005.

[29] 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 Photonics Journal*, vol. 14, no. 1, pp. 1–8, 2022.

[30] W. M. R. Shakir, J. Charafeddine, H. Hamdan, I. A. Al-shabeeb, N. G. Ali, and I. E. Abed, "Security-reliability tradeoff analysis for multiuser FSO communications over a generalized channel," *IEEE Access*, vol. 11, pp. 53 019–53 033, 2023.

[31] *Impact of uplink transmission from fixed service using high altitude platform stations in the 27.5-28.35 GHz and 31-31.3 GHz bands on the Earth exploration-satellite service (passive) in the 31.3-31.8 GHz band*, Rec. ITU-R F.1570-2, International Telecommunication Union, Geneva, Switzerland, 2010.

[32] M. Hess, P. Koepke, and I. Schult, "Optical properties of aerosols and clouds: The software package *OPAC*," *Bulletin of the American Meteorological Society*, vol. 79, no. 5, pp. 831–844, 1998.