

Sensing-Assisted Turbulence-Induced Secret Key Distribution for FSO-based UAV Systems

Luan V. Doan, Hoang D. Le, and Anh T. Pham

Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu 965-8580, Japan

Abstract—This paper proposes a sensing-assisted secret-key generation (SKG) framework for unmanned aerial vehicle (UAV)-based free-space optical (FSO) systems. By exploiting the reciprocity of turbulence-induced channel fluctuations, legitimate users can generate shared secret keys directly from reciprocal FSO channel observations. However, in UAV-FSO links, hovering instability and narrow optical beams introduce pointing errors that impair channel reciprocity and limit the achievable secret-key rate (SKR). To mitigate this issue, optical beam-alignment sensing is performed prior to channel probing to improve alignment accuracy. A beam-alignment-aware time-varying FSO channel model is developed by jointly considering atmospheric turbulence, path loss, beam misalignment due to finite alignment resolution, and temporally correlated pointing errors induced by UAV hovering fluctuations. Based on the resulting reciprocal channel observations, practical SKG procedures, including channel probing, quantization, information reconciliation, and privacy amplification, are incorporated for secure key extraction. Numerical results demonstrate that sensing-assisted beam alignment significantly enhances channel reciprocity, improves raw key generation performance, and increases the achievable SKR under practical UAV-based FSO conditions.

Index Terms—Free-space optics, atmospheric turbulence, sensing, physical-layer security.

I. INTRODUCTION

The evolution of beyond-5G/emerging 6G wireless networks has driven increasing interest in UAV-assisted communication systems for applications such as aerial surveillance, emergency response, and environmental monitoring. Due to their flexible mobility and rapid deployment capability, UAVs are expected to play an important role in future wireless infrastructures. However, the broadcast nature of wireless channels and the dynamic topology of UAV networks also introduce significant security and privacy challenges [1].

Conventional systems mainly rely on public-key cryptography (PKC) for secret-key distribution [2]. However, PKC security relies on computationally hard problems that may become vulnerable to quantum computing, particularly due to algorithms such as Shor's algorithm [3]. Although quantum key distribution (QKD) offers information-theoretic security [4], its practical deployment remains constrained by high hardware complexity, costly quantum devices, and performance degradation under severe channel attenuation [5]. These limitations motivate the development of low-complexity quantum-safe physical-layer secret-key generation techniques.

Among various physical-layer security approaches, key distribution based on channel reciprocity has attracted significant attention [6]. In free-space optical (FSO) systems, atmospheric

turbulence naturally induces random fluctuations in the received optical intensity, which can serve as a common randomness source for legitimate users. By exploiting reciprocal channel observations, legitimate terminals can extract identical secret keys without relying on computationally intensive cryptographic algorithms or dedicated quantum hardware [7]. Existing studies have investigated turbulence-induced SKG in terrestrial FSO systems under various turbulence conditions and eavesdropping scenarios [8]–[11]. While these approaches are effective for static terrestrial FSO systems, extending turbulence-induced SKG to dynamic UAV-based FSO systems introduces significant practical challenges. The UAV hovering-induced pointing misalignment significantly degrades channel reciprocity and reduces the received optical power, thereby limiting the achievable secret key rate (SKR).

Although acquisition, pointing, and tracking (APT) can mitigate pointing misalignment, conventional high-precision APT systems are often bulky, heavy, and power-intensive, making them unsuitable for resource-constrained hovering UAVs. A recent study in [12] has demonstrated that sensing-assisted beam alignment employing LiDAR-like optical scanning technologies can significantly enhance the reliability of UAV-based FSO systems. Nevertheless, the impact of sensing-assisted alignment and residual pointing errors on turbulence-induced SKG performance has not been thoroughly investigated. In particular, the tradeoff between sensing and key generation remains unclear, since longer sensing improves beam alignment and channel reciprocity but reduces the time available for channel probing and key extraction.

This paper proposes a sensing-assisted turbulence-induced secret-key distribution framework for FSO-based UAV systems. Optical sensing is first employed to improve beam alignment prior to channel probing, where the sensing resolution and UAV hovering fluctuations are jointly incorporated into the pointing-error model. Subsequently, temporally correlated atmospheric turbulence is exploited to generate reciprocal channel observations for secret-key extraction. The proposed framework further incorporates practical SKG procedures, including channel probing, quantization, reconciliation, and privacy amplification. Numerical results validate the effectiveness of the proposed system and investigate the tradeoff between sensing and probing time.

The remainder of this paper is organized as follows. Sec. II presents the system architecture, sensing model, and secret-key generation process. Sec. III introduces the proposed time-varying FSO channel model. Numerical results are provided

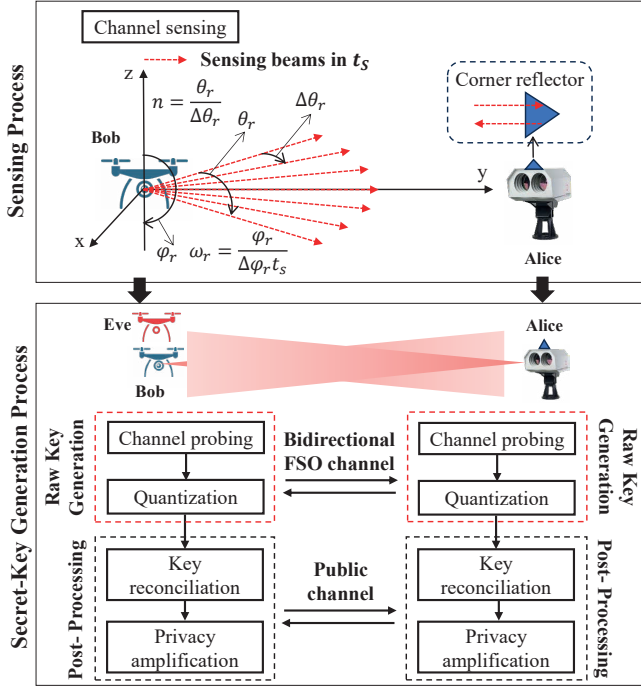


Fig. 1: System Architecture of the Proposed Sensing-Assisted Turbulence-Induced SKG Framework.

in Sec. IV, followed by conclusions in Sec. V.

II. SYSTEM DESCRIPTIONS

We consider a sensing-assisted FSO system in which a hovering UAV and a ground base station perform SKG by exploiting reciprocal channel observations instead of conventional data transmission. The UAV establishes a line-of-sight optical link with the ground node, while sensing and channel probing share the same optical front-end and operate in a time-division manner. Each time slot of duration T is divided into a sensing interval t_s and a probing interval t_p , satisfying $T = t_s + t_p$, where sensing is used to enhance beam alignment and probing is used for reciprocal channel measurements. We emphasize that only sensing and probing are carried over the FSO link, while post-processing steps, including key reconciliation, and privacy amplification are executed over an authenticated public channel. The system architecture is illustrated in Fig. 1.

A. Sensing-Assisted Tracking Model

In the sensing stage, the UAV performs optical beam scanning to estimate the direction of the ground receiver for subsequent beam alignment. To characterize the sensing-induced pointing error, the azimuth and elevation angles are estimated using multi-line and rotational optical scanning methods. Since the communication distance is significantly larger than the typical ranging error, the effect of range estimation uncertainty is neglected and only angular sensing errors are considered. The transmitted scanning beam is reflected

by a corner reflector deployed at the ground receiver and redirected back toward the UAV, where the reflected optical signal is captured by a photodetector (PD) array. The received reflected signal is then utilized to estimate the angle-of-arrival (AOA), thereby enabling accurate angular sensing for beam alignment [12].

In the Cartesian coordinate system, the UAV is located at the origin $(0, 0, 0)$, while the receiver is positioned at $(0, d, 0)$, where the line-of-sight (LOS) direction is aligned with the positive y -axis. Let θ_r denote the horizontal scanning range and n the number of scanning lines. The azimuth-angle resolution is expressed as

$$\Delta\theta_r = \frac{\theta_r}{n}. \quad (1)$$

Similarly, let φ_r denote the vertical scanning range and ω_r represent the scanning frequency. The elevation-angle resolution during the sensing interval t_s is given by

$$\Delta\varphi_r = \frac{\varphi_r}{\omega_r t_s}. \quad (2)$$

Since the ideal LOS direction corresponds to zero azimuth and elevation angles, the residual beam offsets are approximated as

$$\theta \approx \Delta\theta_r, \quad \varphi \approx \Delta\varphi_r. \quad (3)$$

As the optical beam propagates toward the receiver plane located at $y = d$, the beam-center coordinates on the transverse (x, z) plane can be approximated by

$$x = d \tan(\theta) \approx d \Delta\theta_r, \quad (4)$$

$$z = d \tan(\varphi) \sec(\theta) \approx d \Delta\varphi_r. \quad (5)$$

Accordingly, the radial displacement between the beam center and the receiver center is expressed as

$$r = \sqrt{x^2 + z^2} \approx d \sqrt{\Delta\theta_r^2 + \Delta\varphi_r^2}. \quad (6)$$

B. Secret-Key Generation Process

After the channel sensing process, the UAV and the base station proceed with secret-key generation based on reciprocal channel observations. Specifically, the SKG procedure consists of four steps as follows.

Step 1 - Channel Probing: After beam alignment, Alice and Bob exchange optical probing signals over the reciprocal FSO channel during the probing interval $t_p = T - t_s$. The received optical signal at terminal $k \in \{AB, BA\}$ is expressed as

$$r_k(n) = \mathcal{R} P_t h_k(n) + n_k(n), \quad (7)$$

where $\mathcal{R}$ denotes the photodetector responsivity, P_t is the transmitted optical power, $h_k(n)$ denotes the composite FSO channel coefficient, and $n_k(n)$ represents the receiver noise.

Step 2 - Quantization: The received signal observations are converted into binary sequences using a two-threshold lossy quantization scheme [13]. Specifically, the upper and lower quantization thresholds are determined as

$$q_{\pm} = \mu_r \pm \alpha_q \sigma_r, \quad (8)$$

where μ_r and σ_r denote the mean and standard deviation of the received signal samples, respectively, and α_q is the guard-band coefficient.

Based on the received signal observation $r_k[n]$, the generated binary sequence $B[n]$ is expressed as

$$B[n] = \begin{cases} 1, & r[n] > q_+, \\ 0, & r[n] < q_-, \\ \text{discard}, & q_- \leq r_k[n] \leq q_+. \end{cases} \quad (9)$$

Step 3 - Key Reconciliation: Due to noise and channel mismatch, the generated raw keys may contain bit disagreements. To correct these errors, a systematic LDPC code is employed for information reconciliation [14]. Alice computes the syndrome

$$p = xH^T, \quad (10)$$

where $\mathbf{x}$ denotes Alice's raw key vector and H is the LDPC parity-check matrix. The syndrome is then transmitted for key recovery at Bob.

Step 4 - Privacy Amplification: To remove information potentially leaked during public reconciliation, privacy amplification is applied to the reconciled key sequence to generate the final secret key with high secrecy.

III. TIME-VARYING FSO CHANNEL MODEL

A. Temporally Correlated Turbulence Model

Atmospheric turbulence induces random fluctuations in the received optical intensity. To model this effect, a temporally correlated Log-normal fading process is adopted based on experimentally validated APD-based FSO measurements [15].

Particularly, an i.i.d. Gaussian sequence is generated as $z_n \sim \mathcal{N}(0, 1)$, $n = 1, 2, \dots, N$. Then, a temporally correlated Gaussian process $x(n)$ is obtained by passing z_n through a low-pass finite impulse response (FIR) filter characterized by the coherence time.

$$H(f) = \sqrt{\sigma_L^2 \tau_t \sqrt{\pi}} \exp\left(-\frac{1}{2}(\pi \tau_t f)^2\right), \quad (11)$$

where σ_L^2 is the variance of log-amplitude fluctuations defined as $\sigma_L^2 = \ln(1 + \sigma_T^2)$, with σ_T^2 the power scintillation index.

The log-normal turbulence fading coefficient is given by

$$h_t(n) = \exp\left(x(n) - \frac{\sigma_L^2}{2}\right). \quad (12)$$

Also, the autocorrelation function of $x(n)$ is expressed by

$$R_x(\tau) = \sigma_L^2 \exp\left(-\left(\frac{\tau}{\tau_0}\right)^2\right). \quad (13)$$

To model channel reciprocity during bidirectional probing, the forward process $x_{AB}(n)$ is obtained from $x(n)$, while the reverse process is constructed as [16]

$$x_{BA}(n) = \rho_t x_{AB}(n) + \sqrt{1 - \rho_t^2} \tilde{x}(n), \quad (14)$$

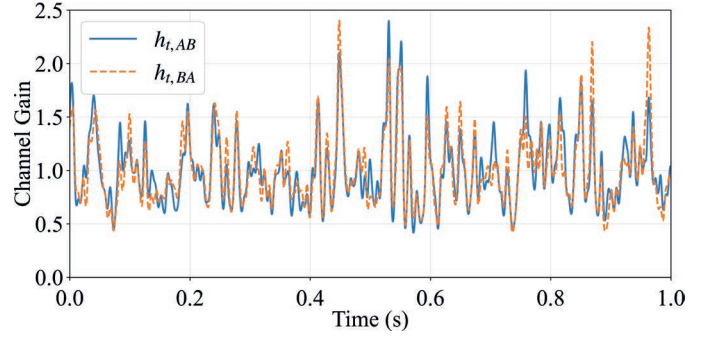


Fig. 2: Forward and reverse turbulence fading realizations over time with $\rho_t = 0.9$.

where $\tilde{x}(n)$ is an independent Gaussian process with identical statistics, and $\rho_t \in [0, 1]$ denotes the turbulence correlation coefficient. The corresponding fading coefficients are given as

$$h_{t,AB}(n) = \exp\left(x_{AB}(n) - \frac{\sigma_L^2}{2}\right), \quad (15)$$

$$h_{t,BA}(n) = \exp\left(x_{BA}(n) - \frac{\sigma_L^2}{2}\right). \quad (16)$$

Figure 2 shows an example regarding forward and reverse turbulence fading realizations for $\rho_t = 0.9$ under a weak turbulence condition with $\sigma_T^2 = 0.1$.

B. Time-Related Pointing Error Channel Model

From the sensing model, the deterministic beam offsets caused by finite sensing resolution are defined as

$$\mu_x = d\Delta\theta_r, \quad \mu_z = d\Delta\varphi_r, \quad (17)$$

where d denotes the transmission distance.

The horizontal and vertical beam-jitter components in both links are modeled as first-order autoregressive (AR(1)) processes [17]. For the link $k \in \{AB, BA\}$, the horizontal and vertical jitter processes are respectively given by

$$x_{j,k}(n) = \alpha_p x_{j,k}(n-1) + \beta_p \sigma_j z_{x,k}(n), \quad (18)$$

$$z_{j,k}(n) = \alpha_p z_{j,k}(n-1) + \beta_p \sigma_j z_{z,k}(n), \quad (19)$$

where $\alpha_p = \exp\left(-\frac{\Delta t}{\tau_p}\right)$ and $\beta_p = \sqrt{1 - \alpha_p^2}$, with τ_p denoting the pointing-error coherence time, Δt the sampling interval, and σ_j the standard deviation of UAV spatial jitter. Moreover $z_{x,k}(n)$ and $z_{z,k}(n)$ being mutually independent Gaussian random variables following $\mathcal{N}(0, 1)$.

In the reverse link, finite sensing resolution introduces deterministic beam offsets in addition to hovering-induced jitter, whereas only hovering-induced jitter is considered in the forward link after beam alignment, i.e.,

$$\delta_k = \begin{cases} 1, & k = BA, \\ 0, & k = AB. \end{cases} \quad (20)$$

The instantaneous beam-center coordinates are expressed as

$$x_k(n) = \delta_k \mu_x + x_{j,k}(n), \quad (21)$$

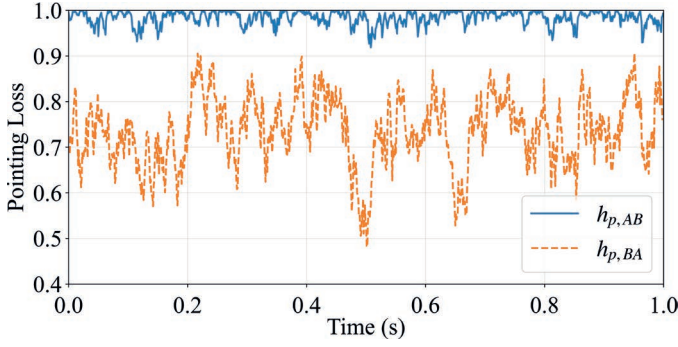


Fig. 3: Forward and reverse pointing-error fading realizations over time.

$$z_k(n) = \delta_k \mu_z + z_{j,k}(n). \quad (22)$$

The corresponding radial displacement is given by

$$r_k(n) = \sqrt{x_k^2(n) + z_k^2(n)}. \quad (23)$$

Assuming a Gaussian beam profile and a circular receiver aperture, the pointing-error fading coefficient is given by [17]

$$h_{p,k}(n) = A_0 \exp\left(-\frac{2r_k^2(n)}{w_e^2}\right). \quad (24)$$

where A_0 denotes the maximum collected power fraction under perfect alignment, and w_e represents the equivalent beam radius at the receiver plane. Here, $A_0 = [\text{erf}(v)]^2$, where $v = \frac{\sqrt{\pi} r_a}{\sqrt{2} w_z}$, while the equivalent beam radius $w_e^2 = w_z^2 \frac{\sqrt{\pi} \text{erf}(v)}{2v \exp(-v^2)}$, with r_a denoting the receiver aperture radius, and w_z is the beam waist radius at the receiver plane.

Figure 3 shows an example regarding the forward and reverse pointing-error fading realizations over time.

C. Combined FSO Channel Model

The composite channel coefficient for the forward or reverse link is given as

$$h_k(n) = h_l h_{t,k}(n) h_{p,k}(n), \quad k \in \{AB, BA\}, \quad (25)$$

where $h_l = \exp(-\kappa d)$ denotes the deterministic atmospheric path loss based on the Beer–Lambert law, with κ being the atmospheric attenuation coefficient and d the propagation distance [18], while $h_{t,k}(n)$ and $h_{p,k}(n)$ represent the turbulence and pointing-error fading components, respectively.

IV. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we evaluate the performance of the proposed sensing-assisted secret-key generation framework for UAV-based FSO systems. The maximum sensing duration is constrained to 50% of the time-slot duration T , where $t_s \leq 0.5T$. The simulation parameters employed in the proposed framework are summarized in Table I. Accordingly, the following results first investigate the impact of sensing and channel conditions on SKR performance as well as different eavesdropping scenarios. Here, SKR is defined as the raw key generation rate.

TABLE I: System Parameters

Parameters	Symbol	Value
Link length	d	2000 m
Transmission power	P_t	60 mW
Beam divergence angle	θ_{div}	1 mrad
Aperture radius	r_a	5 cm
Atmospheric attenuation	h_l	0.9
Turbulence coherence time	τ_t	10^{-3} s
Pointing error coherence time	τ_p	10^{-2} s
Std. dev. of position error	σ_{pf}	3 cm
Time slot duration	T	1 s
Max sensing time ratio	η_{max}	50%
Vertical FOV for sensing	φ_r	0.1 rad
Horizontal FOV for sensing	θ_r	0.1 rad
Scanning frequency	ω_r	1.8×10^3 points/s
Multi-line	n	512

First, Fig. 4 shows the SKR performance versus the sensing duration t_s under different FSO channel conditions. As shown in Fig. 4(a), increasing t_s improves the angular sensing resolution, thereby reducing radial beam misalignment and enhancing the SKR. In addition, larger $\rho_{t,AB}$ further improves the SKR owing to stronger reciprocity between the forward and reverse turbulence channels. Fig. 4(b) reveals that the SKR is degraded when the beam divergence angle θ_{div} is either too small or too large. Specifically, narrow beams are more sensitive to residual pointing errors, whereas wide beams suffer from beam spreading and reduced received optical power, making a moderate beam divergence angle preferable. Finally, Fig. 4(c) shows that the turbulence strength σ_T^2 introduces a tradeoff between channel randomness and reciprocity. While weak turbulence provides insufficient randomness for key generation, excessively strong turbulence increases observation mismatches due to severe fading fluctuations. Consequently, the highest SKR is achieved under moderate turbulence conditions.

Next, Fig. 5 illustrates the SKR performance versus the sensing duration t_s under different Bob–Eve separation distances d_{BE} , assuming perfect turbulence correlation between Alice and Bob, $\rho_{t,AB} = 1$. As shown in Fig. 5(a), the SKR strongly depends on the Bob–Eve channel correlation, where larger $\rho_{t,EB}$ reduces the SKR because Eve observes turbulence-induced channel fluctuations more similar to Bob. Increasing d_{BE} improves the SKR by reducing both the received optical power and channel correlation at Eve. This effect becomes more pronounced in Figs. 5(b) and 5(c), where Eve is located farther from the beam center. Together with the results in Fig. 4(b), these findings highlight the importance of properly selecting the beam divergence angle to balance alignment performance and SKR.

V. CONCLUSION

This paper proposed and investigated a sensing-assisted turbulence-induced secret-key generation framework for UAV-based FSO systems. By incorporating sensing resolution, atmospheric turbulence, and UAV-induced pointing errors into a

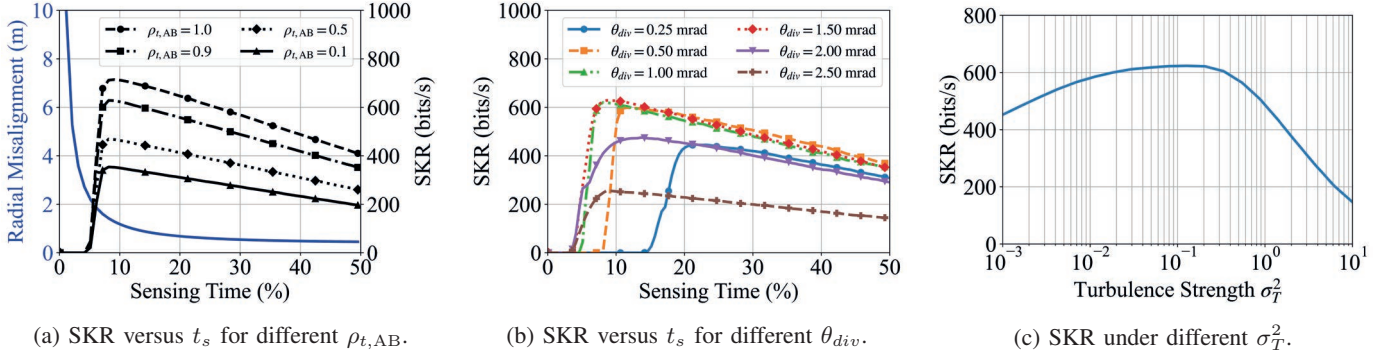


Fig. 4: SKR performance versus sensing time per time slot under various FSO channel conditions.

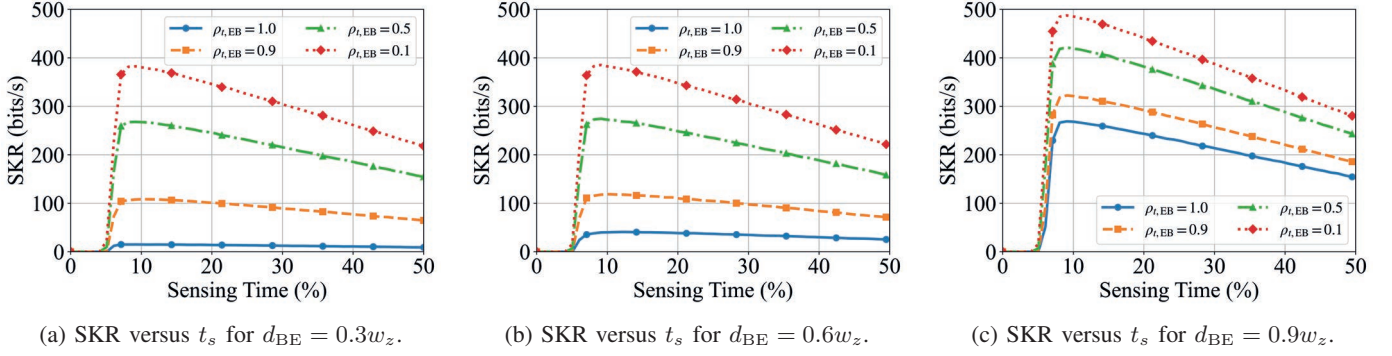


Fig. 5: SKR performance versus sensing time per time slot under different d_{BE} and $\rho_{t,EB}$.

unified time-varying channel model, the impact of beam alignment on secret-key generation was characterized. Numerical results showed that sensing-assisted alignment significantly improves channel reciprocity and the achievable secret-key rate, demonstrating its effectiveness for practical and secure UAV-based FSO communications.

REFERENCES

- [1] W. Zhao *et al.*, "A survey on DRL-based UAV communications and networking: DRL fundamentals, applications and implementations," *IEEE Commun. Surveys Tut.*, vol. 28, pp. 3911–3941, Thirdquarter 2026.
- [2] P. Sharma *et al.*, "Quantum key distribution secured optical networks: A survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2049–2083, Aug. 2021.
- [3] K. Oonishi and N. Kunihiro, "An evaluation of computational complexity of shor's algorithm on surface codes for factorization," *IEEE Access*, vol. 14, pp. 27 264–27 289, Feb. 2026.
- [4] I. B. Djordjevic, "Joint QKD-post-quantum cryptosystems," *IEEE Access*, vol. 8, pp. 154 708–154 712, Aug. 2020.
- [5] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the Qinternet," *IEEE Commun. Surveys Tut.*, vol. 24, no. 2, pp. 839–894, 2022.
- [6] S. Nitinawarat and P. Narayan, "Secret key generation for correlated gaussian sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, Jun. 2012.
- [7] D. Giggenbach, W. Cowley, K. Grant, and N. Perlot, "Experimental verification of the limits of optical channel intensity reciprocity," *Applied Optics*, vol. 51, no. 16, pp. 3145–3152, 2012.
- [8] I. B. Djordjevic, "Atmospheric turbulence-controlled cryptosystems," *IEEE Photon. J.*, vol. 13, no. 1, pp. 1–9, Feb. 2021.
- [9] H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, T. Ito, R. Shimizu, M. Takeoka, and M. Sasaki, "Free space optical secret key agreement," *Opt. Express*, vol. 26, no. 18, pp. 23 305–23 332, Sep 2018.
- [10] 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.
- [11] C. Chen and Q. Li, "Enhanced secret-key generation from atmospheric optical channels with the use of random modulation," *Optics express*, vol. 30, no. 25, pp. 45 862–45 882, 2022.
- [12] Y. Li, L. Wu, Z. Zhang, J. Dang, B. Zhu, X. Zhang, and Y. Wu, "Sensing assisted optical wireless communication for uavs," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 12, pp. 18 620–18 634, 2024.
- [13] A. D. Alshamdayn and M. Min, "A survey of quantization techniques for physical layer-based secret key generation in iot systems," in *2024 IEEE International Conference on Computing (ICOCO)*. IEEE, 2024, pp. 36–41.
- [14] I. B. Djordjevic, "Joint qkd-post-quantum cryptosystems," *IEEE Access*, vol. 8, pp. 154 708–154 712, 2020.
- [15] S. Galijasevic, J. Luo, D. Divsalar, and R. Wesel, "Channel-prediction-driven rate control for ldpc coding in a fading fso channel with delayed feedback," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 3320–3331, 2025.
- [16] D.-J. Jwo, T.-S. Cho, and A. Biswal, "Geometric insights into the multivariate gaussian distribution and its entropy and mutual information," *Entropy*, vol. 25, no. 8, p. 1177, 2023.
- [17] S. W. Sun and J. H. Noh, "End-to-end performance analysis of ccscs o3k optical communication system under atmospheric turbulence and pointing errors," *Aerospace*, vol. 12, no. 10, p. 869, 2025.
- [18] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *Journal of Lightwave technology*, vol. 25, no. 7, pp. 1702–1710, 2007.