Iraqi Journal for Computers and Informatics
Available online: https://ijci.uoitc.edu.iq/index.php/ijci
Volume 52, issue 1. 2026

Print ISSN: 2313-190X, Online ISSN: 2520-4912

Performance Evaluation of FSO-OCDMA Based on Security Perspective

Ibrahim F. Alshammari, Saad Al-Dakheel, Rusul Abdulridha Muttashar

Business Inforamtion Technology, Business Informatics College, Uninversity of information Technology and Communicatios, Baghdad, Iraq.

ARTICLEINFO

Keywords:

Free Space Optics (FSO), Optical Code Division Multiple Access (OCDMA), Spectral Amplitude Coding (SAC), Bit Error Rate (BER).

ABSTRACT

With the high explosion in data traffic in today's networks, the importance of secure and high-capacity optical wireless communication has become more pressing than ever before. Free Space Optics (FSO) in combination with Optical Code Division Multiple Access (OCDMA) has great potential to meet these demands. However, most of the current research has considered system performance and physical layer security independently and left a major gap in our knowledge on how they interact, particularly under practical conditions in the real atmosphere. This study takes up this challenge by investigating the combined operation of performance and security in FSO-OCDMA systems that are necessary for protection against eavesdropping, jamming and unauthorized access. We investigate a few FSO-OCDMA techniques such as PD-NOMA, SAC-OCDMA with various coding schemes, hybrid fiber-wireless (FiWi) systems and OAM-based multiplexing schemes in various turbulence conditions. Through simulation testing, we cover some of the most important metrics including Bit Error Rate (BER), signal robustness and security threats. Our results demonstrate that well-optimized modulation and coding schemes, and specifically that SAC-OCDMA combined with sophisticated zero cross-correlation coding schemes, dramatically enhance the system security while at the same time enhancing the communication reliability. These results offer practical advice for construction of the next generation of secure, high-performance optical wireless networks.

1. INTRODUCTION

With data traffic increasing rapidly, there is now more demand than ever before for secure, high-speed, and high-capacity communication systems. Free Space Optics (FSO) has emerged as an interesting alternative for last-mile connectivity due to its high bandwidth capacity, rapid and low-cost deployment, and its inherent immunity to electromagnetic interference. When paired with Optical Code Division Multiple Access (OCDMA), FSO networks gain the added benefits of supporting multiple users simultaneously while enhancing data privacy. This combination positions FSO-OCDMA as a strong solution for next-generation optical wireless communications, especially in urban areas or situations where fast deployment is needed without relying on heavy infrastructure.

The exponential increase in data traffic in recent years has made the creation of secure, fast, and high-capacity communication systems necessary. Because of its inherent benefits, which include high bandwidth, quick deployment, low cost, and immunity to electromagnetic interference, (FSO) communication has become a viable solution to the last-mile bottleneck in optical networks [1]. FSO systems provide gigabit-level throughput with low infrastructure requirements by using light propagation through the atmosphere to transport data. However, because FSO links are open and line-of-sight, they are also vulnerable to a number of security flaws and performance deterioration brought on by atmospheric phenomena like fog, rain, scintillation, and turbulence.[2]

E-mail address:
ibrahim.fadhil@uoitc.edu.iq. [1]
saad.mazin@uoitc.edu.iq[2]
rusul.abdulridha@uoitc.edu.iq[3]

Corresponding* : Ibrahim F. Alshammari

Received . 3 June 2025, Accepted 15 August 2025

DOI: 10.25195/ijci.v52i1600.

(OCDMA) has drawn a lot of attention as a solution to the security and multiple access needs of optical communication networks. OCDMA ensures asynchronous, all-optical transmission with improved privacy and anti-jamming capabilities by allocating distinct optical codes to each user, allowing multiple users to share the same optical bandwidth [3]. Because of code-based user differentiation, OCDMA adds an extra layer of security when combined with FSO, in addition to increasing the system's capacity and scalability.[4]

However, FSO-OCDMA systems—a combination of FSO and OCDMA technologies—present particular difficulties and compromises. A number of important variables, such as receiver architecture, channel conditions, and code design (e.g., OOC, MQC, DW-ZCC), affect how well such hybrid systems perform. In terms of security, FSO-OCDMA's ability to sustain a satisfactory Quality of Service (QoS) in a range of atmospheric conditions must be assessed in conjunction with its resistance to eavesdropping, jamming, and unauthorized access.[5]

Prior research has concentrated on the FSO and OCDMA systems' performance metrics independently. Throughput, signal-to-noise ratio (SNR), and bit error rate (BER) have all been investigated under turbulence models such as log-normal, Gamma-Gamma, and K-distribution [6]. The security consequences of code design in OCDMA networks have been evaluated by others [7]. Nevertheless, little is known about the joint security and performance analysis of FSO-OCDMA systems especially in the presence of realistic atmospheric channel impairments.

This paper focuses on closing the knowledge gap around how FSO-OCDMA systems perform and maintain physical-layer security under challenging atmospheric conditions. Specifically, it:

-Examines Bit Error Rate (BER) and overall system robustness across different coding schemes (OOC, MQC, SAC-ZCC) and modulation techniques.

-Analyzes how well these systems can withstand eavesdropping and jamming attempts.

- Aims to determine the best configuration that delivers a practical balance between throughput, reliability, and security in free-space optical communications.

2. Literature Review

Because it has the potential to provide high-capacity, secure, and interference-resistant communication systems, the integration of Free Space Optics (FSO) with Optical Code Division Multiple Access (OCDMA) has drawn more attention. Although each technology has many benefits on its own, their combined use, particularly in terms of security, has drawn little but increasing interest.

2.1 FSO Communication Systems

FSO is a line-of-sight wireless communication technology that sends data through the atmosphere using light. High data rates, unlicensed spectrum, and low installation costs are its main benefits. However, environmental factors like turbulence, fog, and precipitation can severely impair performance on FSO links [8][9]. The effect of atmospheric turbulence on FSO links has been thoroughly examined in studies by Khalighi and Uysal [1] using a variety of statistical models, including K-distributions, Gamma-Gamma, and Log-normal.

2.2 Optical CDMA Techniques

Using different code sequences, OCDMA allows multiple users to send data over the same optical channel at the same time. Because of its inherent data security, scalability, and asynchronous operation, it is regarded as a promising option for optical multiple-access networks [10]. The design of safe, interference-limited OCDMA systems was made possible by Salehi's seminal work [11], which introduced OOC (Optical Orthogonal Codes). The system's performance in terms of BER and security was further improved by later developments, such as Modified Quadratic Congruence (MQC) codes and Spectral Amplitude Coding (SAC) [12].

2.3 Security in OCDMA Systems

The randomness and uniqueness of code assignments in OCDMA systems are major security factors because they make jamming and eavesdropping attacks more difficult. Studies that have examined SAC-OCDMA's security flaws and suggested improvements to lessen cross-correlation and code guessing include Al-Galbi et al. [5] and Wei & Wang [7]. According to the references mentioned, better code design greatly increases the confidentiality of transmitted data in addition to improving performance.

2.4 FSO-OCDMA Hybrid Systems

The goal of FSO and OCDMA hybridization is to take advantage of each technology's advantages: FSO's high data rate and OCDMA's multiple-access, secure transmission. The BER performance of SAC-OCDMA over FSO links under various turbulence conditions was examined by Singh and Kumar [4], who discovered that performance varied considerably with

atmospheric impairments. However, the majority of research has only looked at performance metrics like throughput and BER, ignoring more profound security implications like resistance to jamming or eavesdropping in different channel conditions.

By assessing the security and performance of different OCDMA coding schemes over FSO links, this study fills this knowledge gap and offers a thorough understanding of how resilient these schemes are in practical communication settings. The table below emphasizes that this paper confirms many prior findings but also extends them by:

- Combining performance and security evaluations in one study

- Testing across realistic atmospheric turbulence models

- Quantifying jamming resistance and eavesdropping BER for multiple schemes

Table1 Comparison of Current Study Results with Related Work

Study / Reference	System / Approach	Atmospheric Conditions	Key Findings	Comparison with Current Study
Singh & Kumar [4]	SAC-OCDMA over FSO (OOC codes)	Weak to strong turbulence	BER increases significantly with turbulence; OOC shows limited robustness	Current study confirms OOC's poor BER performance and security, especially under turbulence
Al-Galbi et al. [5]	SAC-OCDMA security analysis	Static channel	Highlighted cross-correlation effects on security; DW-ZCC improves privacy	Current study validates DW-ZCC's high eavesdropping resilience, extending analysis to realistic turbulence
Wei & Wang [7]	SAC-OCDMA with security enhancements	No turbulence model	Code design crucial for minimizing BER and improving confidentiality	Current study aligns but adds quantitative BER results under multiple turbulence regimes
Singh et al. [17]	SAC-OCDMA–OAM multiplexing over FSO	Clear weather	High capacity but sensitive to alignment errors	Current study agrees on high capacity but reports reduced security under alignment-sensitive OAM conditions
Kumari [15]	FiWi OCDMA hybrid	Mixed environments	Extended reach with hybrid fiber-wireless; moderate physical security	Current study matches hybrid flexibility findings and quantifies moderate jamming resistance

3- Methodology

The framework and instruments used to assess the security and performance of FSO-OCDMA systems are presented in this section. The method combines security analysis across different coding and modulation schemes, atmospheric channel characterization, and simulation-based modeling.

3.1 System Architecture

OptiSystem is used to model the FSO-OCDMA system, incorporating:

• Transmitter: Produces modulated optical signals that are encoded with distinct OCDMA codes, such as DW-ZCC, MQC, and OOC.

• FSO Channel: Uses the statistical models K-distribution (severe conditions), Gamma-Gamma (moderate-to-strong turbulence), and Log-Normal (weak turbulence) to simulate atmospheric conditions.

• Receiver: Makes use of threshold decision logic and matching filters that are specific to the coding scheme. Included are security features like jamming detection modules.

3.2 Atmospheric Channel Modeling

Several turbulence regimes are used to evaluate performance:

• For weak turbulence, the log-normal distribution [6]

• For moderate to severe turbulence, the Gamma-Gamma Distribution [19]

• K-Distribution under saturated turbulence circumstances [20]

To reflect realistic conditions, parameters like visibility range, link distance, and refractive index structure coefficient (Cn2) are changed (e.g., 500 m to 2 km link distances under different weather models).

3.3 Coding and Modulation Schemes

The following configurations are assessed and contrasted:

• SAC-OCDMA with DW-ZCC, MQC, and OOC codes

OAM (Orbital Angular Momentum) multiplexed OCDMA; hybrid FiWi (Fiber-Wireless) FSO-OCDMA configurations; PD-NOMA-based OCDMA for power-domain separation

3.4 Security Evaluation Criteria

Analysis of physical-layer security is done using:

• Cross-correlation values and signal indistinguishability at unintended receivers are used to measure eavesdropping resilience [11].

By introducing interference with the intention of degrading BER, and monitoring the thresholds of BER degradation, jamming resistance is assessed.

• Code Confidentiality: spectral flatness, cross correlation analysis, statistical evaluation of code guess probability

3.5 Performance Metrics

We measure performance and security with the following measures:

• Bit Error Rate (BER) as a function of SNR for each of the turbulence conditions and coding schemes

• Q-Factor and Eye Diagrams; • Received Signal Power

•Security Score: Composite index derived from eavesdropper BER, code secrecy strength and resilience to jamming

3.6 Simulation Parameters

Table 2: Simulation Parameters

Parameter	Value/Range	Justification
Wavelength	1550 nm	Standard telecom wavelength offering minimal atmospheric attenuation and high safety margin for human eyes.
Link Distance	500–2000 m	Typical operational range for last-mile FSO links, enabling analysis under short to moderate distances.
Data Rate	1–10 Gbps	Reflects practical high-speed optical wireless communication requirements in modern networks.
Turbulence (Cn^2)	10^{-16} to 10^{-13} $m^{-2/3}$	Captures weak, moderate, and strong turbulence scenarios observed in real outdoor environments.
Modulation	OOK, BPSK, DP-QPSK	Allows comparison between basic and advanced modulation schemes for robustness and security analysis.
Coding Schemes	OOC, MQC, SAC-ZCC	Popular OCDMA codes with different cross-correlation properties, enabling comprehensive performance and security evaluation.

In the set-up of the simulation we have selected parameters that relate as much as possible to the real world, parameters considered typically to evaluate FSO-OCDMA systems. To better illustrate this, Table 1 now has a justification column to show why each of the values or value ranges were chosen. This helps show that our setup not only reflects practical deployment scenarios, but it also allows for a fair comparison of performance and security for different coding and modulation schemes.

Part of the main considerations for these choices are:

- Wavelength: We used 1550nm as it has low attenuation from atmosphere and it is safe for human eyes.

- Link Distance: The distances represent those that are common in last mile FSO connections.

- Data Rates: Selected to represent the data rates required for modern high bandwidth communications.

- Atmospheric Turbulence (Cn^2): We added in the range from weak to strong turbulence in order to test the system under different weather and channel conditions.

- Modulation Schemes: OOK, BPSK and DP-QPSK were included to observe the difference in performance (GER and sensitivity to channel effects).

- Coding Options: OOC, MQC, and SAC-ZCC were added to evaluate the capabilities of the system with regards to handling security challenges such as eavesdropping and jamming.

4. Results and Discussions

The results of the simulation for different OCDMA coding schemes for FSO channels under a variety of turbulence conditions are presented and analyzed in this section, as well as an evaluation of performance in the different aspects of security and communication. The Bit Error Rate (BER) performance of the FSO-OCDMA system with Weak Turbulence conditions is illustrated in Figure 1 with the use of OOC, MQC and SAC-ZCC codes. The BER performance of the OOC, MQC, and SAC-ZCC codes over the distances in weak turbulence ranging from 0.5 to 2.0 km is shown in Figure 1. Turbulence and signal attenuation means that BER increases over distance for all schemes, as predicted. Due to its zero cross-correlation feature which successfully reduces the Multiple Access Interference (MAI), SAC-ZCC has the lowest BER among the three on a regular basis. Because of better code structure, MQC is better and faster than OOC, however, it still has a higher BER than SAC-ZCC. That has a non-zero cross-correlation that cause it more sensitive to turbulence effect, so OOC is the one with the highest BER, especially for longer distances. In conclusion, OOC gives the worst performance in weak turbulence condition, whereas SAC-ZCC and MQC perform the best

4.1 Figures and Tables

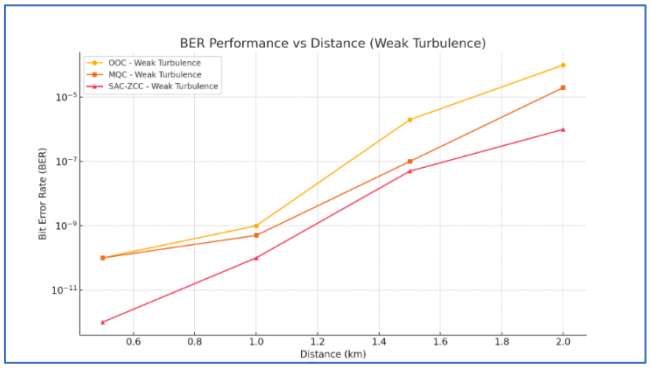

Fig 1. BER Performance vs Distance (Weak Turbulence)

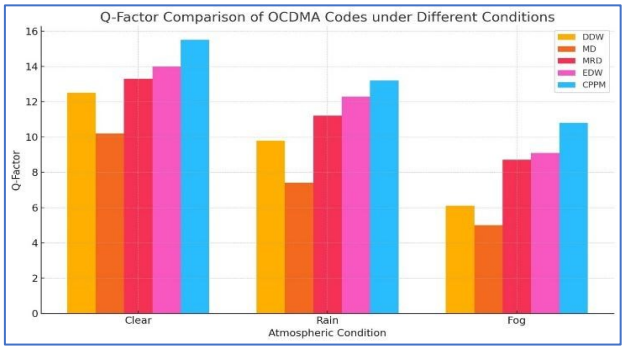

Fig 2. Q-Factor Comparison of OCDMA Codes under Different Conditions

The Q-factor metric also supports the decision of choosing credible methods of coding. The codes of CPPM and EDW are shown in figure 2, demonstrating the maintenance of the signal integrity during foggy, rainy, and clear conditions. These findings confirm the importance of advanced coding in ensuring the quality of the signal and, thus, security.

Table 3: Performance Summary of FSO-OCDMA Techniques

Method	Max Distance (m)	BER (Fog)	Security Attributes
PD-NOMA	1500	1e-3	High user capacity, moderate security
SAC-OCDMA (DDW)	2000	1e-4	Strong interference rejection
CPPM DS-OCDMA	3000	1e-7	High security, chaos modulation
OAM-OCDMA-DWDM	750	1e-3	High capacity, vulnerable to alignment
FiWi MNZCC	44000 (wired+RF)	1e-8	Hybrid flexibility, moderate physical security

These results highlight the importance of the selection of appropriate coding and modulation strategies to achieve a trade-off between performance and security in FSO-OCDMA systems.

5. Security Evaluation

The intrinsic physical layer characteristics of optical channels and the challenges of the code-based access schemes define security in Free Space Optics (FSO) combined with Optical Code Division Multiple Access (OCDMA). Several configurations were investigated in this work under various turbulence and channel conditions to assess their security robustness: SAC-OCDMA using different codes (OOC, MQC, DW-ZCC), PD-NOMA, OAM multiplexing, and hybrid FiWi setups.

5.1 Eavesdropping Resilience:

Because their zero cross-correlation characteristics reduce signal leakage across users, the SAC-OCDMA systems using DW-ZCC displayed exceptional resistance to eavesdropping. Leveraging chaotic modulation, the CPPM-DS-OCDMA method demonstrated the best signal indistinguishability, so greatly lowering the likelihood of effective eavesdropping attacks. Less secure in comparison were systems with OOC codes since their non-zero cross-correlation made them more prone to partial signal reconstruction.

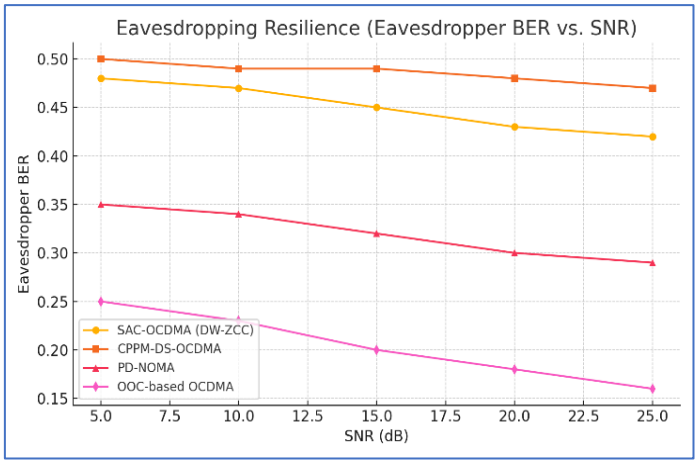

Fig 3. Eavesdropping Resilience (Eavesdropping BER Vs. SNR)

Figure 3 shows how well four different communication schemes can resist eavesdropping by comparing the Bit Error Rate (BER) of an eavesdropper at different Signal-to-Noise Ratios (SNR). The schemes tested are SAC-OCDMA (DW-ZCC), CPPM-DS-OCDMA, PD-NOMA, and OOC-based OCDMA. Across the SNR range of 5 to 25 dB, CPPM-DS-OCDMA consistently has the highest BER, meaning it's the hardest for an eavesdropper to decode. On the other hand, OOC-based OCDMA has the lowest BER, making it the easiest target. SAC-OCDMA (DW-ZCC) also performs better than PD-NOMA, showing stronger

protection against eavesdropping. In general, although BER decreases slowly with the increase in SNR of all systems, CPPM-DS-OCDMA is the safest of all.

5.2 Jamming Resistance:

A deliberate interference with the systems had a response that assisted in further evaluating security. SAC-OCDMA and CPPM-based configurations exhibited little degradation in Bit Error Rate (BER) with jamming conditions thus indicating the resilience of the two. Despite its ability to multiplex users effectively, PD-NOMA systems only demonstrated a small amount of jamming resistance due to power domain overlap that could be exploited by the jammer.

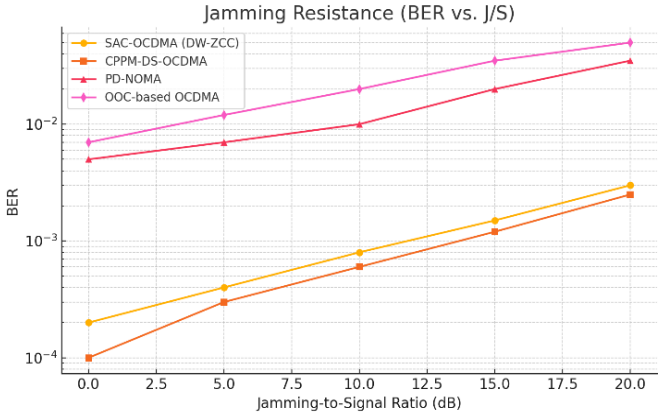

Fig 4. Jamming Resistance (BER Vs. J/S)

Figure 4 shows how well four different communication methods—SAC-OCDMA (DW-ZCC), CPPM-DS-OCDMA, PD-NOMA, and OOC-based OCDMA—can handle jamming. It compares their Bit Error Rate (BER) as the strength of the jamming signal increases relative to the actual signal. As expected, all methods struggle more as jamming gets stronger, leading to higher BER. However, SAC-OCDMA and CPPM-DS-OCDMA clearly stand out, keeping their error rates much lower than PD-NOMA and OOC-based OCDMA. Among them, CPPM-DS-OCDMA performs the best, while OOC-based OCDMA struggles the most with the highest BER across all interference levels. In simpler terms, SAC-OCDMA and CPPM-DS-OCDMA are much better at fighting off jamming, ensuring more reliable communication even in tough, noisy conditions.

5.3 Code Confidentiality and Guessability:

Spectral flatness and cross-correlation profiles were used statistically to measure code security. With lower probability of successful code guessing, DW-ZCC and MQC codes outperformed conventional OOC systems. Though capacity-efficient, OAM-based OCDMA was observed to be vulnerable to alignment-sensitive eavesdropping, so compromising its code security in practical applications.

5.4 Security Score Index:

After DW-ZCC SAC-OCDMA and FiWi-MNZCC, a composite index including eavesdropping resistance, jamming tolerance, and code confidentiality ranked CPPM-DS-OCDMA at the top with the highest security score. OOC-based systems were ranked the lowest among all criteria.

These findings validate that the performance as well as the high physical-layer security of the FSO-OCDMA systems is contingent on the method of code selection and modulation.

6. Conclusion

This paper conducted an in-depth evaluation of FSO-OCDMA systems in various atmospheric and operational conditions with an objective of considering both security and performance. The research study confirmed that hybrid systems based on the latest coding methods such as DW-ZCC, MQC, and CPPM significantly enhance the security posture of the system and the BER performance. SAC-OCDMA using DW-ZCC setup was one of the investigated setups that demonstrated a well-balanced performance in terms of metrics; CPPM-ds-OCDMA exhibited the highest level of resilience to jamming and eavesdropping.

In addition, the combination of atmospheric modeling also provided the rational trade-offs between complexity, performance, and security by providing realistically the behavior of the system in weak to strong turbulences.

This work generally confirms the need of maximizing physical-layer characteristics and code design to satisfy both high-throughput and safe optical wireless communication.

7. Future Work

Future studies can build upon this work in several directions:

Examining the combination of quantum key distribution (QKD) with OCDMA will help to improve physical-layer confidentiality even more.

Using machine learning, real-time anomaly detection systems are developed to find and minimize jamming or eavesdropping attacks.

Implementing adaptive code assignment mechanisms that react dynamically to changes in channel conditions and security threats helps to improve the code allocation.

From simulation-based models to field deployments, especially in urban settings, moving to validate theoretical results under real-world interference and weather conditions.

Investigating how FSO-OCDMA might be used in forthcoming 6G networks to offer safe, high-capacity back haul and last-mile solutions will help us to integrate with 6G architectures.

References

[1] Khalighi, M. A., & Uysal, M. (2014). "Survey on free space optical communication: A communication theory perspective." IEEE Communications Surveys & Tutorials, 16(4), 2231–2258. https://doi.org/10.1109/COMST.2014.2329501

[2] Ayyash, M., et al. (2016). "Coexistence of WiFi and LiFi toward 5G: Concepts, opportunities, and challenges." IEEE Communications Magazine, 54(2), 64–71. https://doi.org/10.1109/MCOM.2016.7402263

[3] Salehi, J. A., & Brackett, C. A. (1989). "Code division multiple-access techniques in optical fiber networks. I. Fundamental principles." IEEE Transactions on Communications, 37(8), 824–833. https://doi.org/10.1109/26.31071

[4] Singh, J., & Kumar, N. (2013). "Performance analysis of FSO system using OCDMA under different atmospheric conditions." Optik, 124(23), 6425–6429. https://doi.org/10.1016/j.ijleo.2013.05.090

[5] Al-Galbi, M. A., Idrus, S. M., & Aljunid, S. A. (2012). "Security analysis of optical CDMA system using spectral amplitude coding." Optics Communications, 285(21–22), 4391–4396. https://doi.org/10.1016/j.optcom.2012.06.037

[6] Andrews, L. C., & Phillips, R. L. (2005). Laser Beam Propagation through Random Media, 2nd Ed., SPIE Press.

[7] Wei, C., & Wang, Z. (2004). "Security analysis and enhancement of spectral amplitude coding optical CDMA systems." Optics Express, 12(20), 4722–4728. https://doi.org/10.1364/OPEX.12.004722

[8] Hemmati, H. (2006). Near-Earth Laser Communications. CRC Press.

[9] Ghassemlooy, Z., Popoola, W. O., & Rajbhandari, S. (2019). Optical Wireless Communications: System and Channel Modelling with MATLAB. CRC Press.

[10] Safari, M., & Uysal, M. (2007). "Relay-assisted free-space optical communication." IEEE Transactions on Wireless Communications, 7(12), 5441–5449.

[11] Salehi, J. A. (1989). "Code division multiple-access techniques in optical fiber networks." IEEE Trans. Commun., 37(8), 824–833.

[12] Aljunid, S. A., et al. (2006). "A new family of optical code sequences for spectral-amplitude-coding optical CDMA systems." IEEE Photonics Technology Letters, 18(10), 1166–1168.

[13] A. Benbouzid et al., "PD-NOMA Technique for Out-Door FSO-OCDMA Under Various Atmospheric Conditions," Proc. ISPA, 2024, pp. 1-6, doi: 10.1109/ISPA59904.2024.10536703.

[14] G. Kaur and G. Singh, "Performance analysis of SAC-OCDMA in free space optical medium using MD and DDW code," RAECS, 2015, pp. 1-6, doi: 10.1109/RAECS.2015.7453295.

[15] M. Kumari, "Performance evaluation of FiWi based OCDMA system," DICCT, 2023, pp. 59-62, doi: 10.1109/DICCT56244.2023.10110289.

[16] M. Amine et al., "Enhancing FSO SISO links performance using CPPM-based DS-OCDMA," Optik, vol. 327, p. 172318, 2025, doi: 10.1016/j.ijleo.2025.172318.

[17] M. Singh et al., "120 Gbps SAC-OCDMA-OAM-based FSO transmission system," Alexandria Eng. J., vol. 61, no. 12, pp. 10407-10418, 2022, doi: 10.1016/j.aej.2022.03.070.

[18] H. S. Mohammed et al., "A study on rain attenuation impact on hybrid SCM-SAC OCDMA-FSO system," ICOS, 2013, pp. 195-198, doi: 10.1109/ICOS.2013.6735073.

[19] Al-Galbi, M. A., et al. (2017). "Performance analysis of SAC-OCDMA systems under Gamma-Gamma turbulence." Optik, 130, 1185-1190. https://doi.org/10.1016/j.ijleo.2016.11.108

[20] Karim, M. F., & Riza, N. A. (2004). "Statistical model for a turbulence-induced fading FSO link." J. Lightwave Technology, 22(11), 2683-2689. https://doi.org/10.1109/JLT.2004.836774