**International Journal of Engineering Research and Reviews** ISSN 2348-697X (Online)
Vol. 12, Issue 3, pp: (150-180), Month: July - September 2024, Available at: www.researchpublish.com

# A Comprehensive Review on Security in Free Space Optical Communication

Shreya S. Patil[1], Chinchu Joseph[2], D. T. Varpe[1], A. A. Bazil Raj[2]

[1]Electronics and Telecommunication Department, Pune Vidyarthi Griha's College of Engineering and Technology and G.K. Patel (Wani) Institute of Management, Vidyanagari, Parvati, Pune, Maharashtra, India, 411009

[2]RF Photonics Laboratory, Defence Institute of Advanced Technology, Girinagar, Pune, Maharashtra, India, 411025

**DOI: https://doi.org/10.5281/zenodo.13851700**

**Published Date: 27-September-2024**

***Abstract:*** **Free Space Optical (FSO) Communication is an optical communication technology that uses laser beams to wirelessly transmit data over free space. It is a prominent and essential technology in wireless communication. It is an in-demand technology for wireless communication as it has high data rate transmission capacity, high bandwidth, low latency, and lower power consumption. FSO Communication is very advantageous in regards to security in the communication technology. Even then issues with respect to security persists as there is advancement in different technologies. FSO systems are still vulnerable to eavesdropping, jamming and physical layer attacks as it utilizes open Line of Sight (LoS) communication. Several extensive studies have been conducted to improve the security measures in FSO Communication. This review studies the current scenarios in security of FSO communication. This paper reviews several work conducted on security in FSO aims to provide a comprehensive review of existing security strategies, compare their effectiveness, and highlight key research gaps that need to be addressed for future developments in secure FSO communication.**

***Keyword:*** **FSO Communication, Optical Wireless Communication (OWC), Security in FSO Communication, Physical Layer Security, Encryption Techniques, QKD.**

## I. INTRODUCTION

In the new era of communication, with the need for high-speed and broad bandwidth, Free Space Optical (FSO) Communication, also known as Unguided Optical Communication (UOC) [1,2], is in high demand surpassing traditional Radio Frequency (RF) systems. FSO communication utilizes light rays, using lasers, to transmit data through free space (air as medium) at very high speed. It has several advantages over traditional RF systems which have many limitations like lesser bandwidth, power consumption, narrow band of frequency on suitable electromagnetic spectrum, expense of installation and maintenance, while FSO systems use optical spectrum giving access to a much broader bandwidth [3]. Even compared to fiber optic communication, FSO is preferable because of its significantly lesser initial investment need, broad bandwidth, high speed, faster deployment and easily upgradeable technology [4]. FSO with its utilization of optical signals, is more secure with respect to electromagnetic interference, therefore resulting in more reliable data transmission. These advantages of FSO technology makes it a very sought-after solution in a range of applications, such as Optical Wireless Home Network, Optical Wireless Terrestrial Network, Optical Wireless Satellite Network [5]. It can be deployedin densely populated areas without any need for extensive cabling for various applications like indoor WLAN, outdoor wireless access, mobile cellular networks, last-mile access, point-to-point links [6, 7]. FSO is preferred for inter-satellite communication with its many advantages over RF, such as high data rates over long distances, smaller antenna sizes, and lower transmit power, narrower beams resulting in no interference and better security [8].

Despite all the advantages, FSO communication systems deployment is with formidable difficulties, mostly linked to security. In this aspect, the FSO links are highly vulnerable to a large number of security threats because of their open-air nature. Unlike RF communications that can partially depend on walls and buildings as a physical barrier, FSO signals find their way through the atmosphere in a straight line of sight. This openness opens up vulnerabilities to eavesdropping, signal jamming, and denial-of-service attacks. For instance, any adversary who has access to the optical beam path might

intercept or block the transmission, thus comprising the confidentiality, integrity, and availability of the communication link. One major challenge to securing FSO communications lies in the special characteristics of optical signal propagation. Signal degradations can also occur due to atmospheric turbulence, rain, fog, and dust [9]. A part of this degradation of communication performance can create new vectors for attacks. For instance, opponents may hijack or exploit the perturbation introduced by atmospheric perturbations, achieving increased error rates or making the system break down in such a way that it yields a complete breakdown of the communication link. In addition, precise beam alignment is critical in FSO systems: Even minor misalignments can result in large signal loss, and the adversaries can exploit this by deliberately creating misalignment using physical interference [10-13]

Apart from such environmental and physical problems, another complication that exists in deploying FSO communication in critical infrastructures is the current lack of standardized security protocols custom-made for it. While traditional encryption techniques designed for RF systems are aimed at different threats than those unique to FSO systems, they alone may not be sufficient in each case of high data rates and low latency requirements common in so many FSO applications. Being very important, this layer of security has to be complemented by some other security measures at the physical and network layers to provide full protection against possible security threats [9, 14]. New emerging technologies, such as quantum key distribution, offer theoretically unbreakable security by applying principles of quantum mechanics [15]. However, the real integration of these technologies into practical FSO systems are still to be explored sufficiently. Since the applications of FSO technology are growing rapidly in military communication, smart city infrastructure, and disaster recovery networks, the security issues mentioned above have become very significant and are growing in importance. Such a security breach in these applications may have enormous effects: from unauthorized disclosures of sensitive information to disruption of key communication networks. Therefore, to allow for an adequate andsecure functioning of FSO systems in the present and future deployments, there is a need to understand the landscape of security in FSO communication.

This review paper presents the overview of security challenges associated with FSO communication systems. It introduces the basic concepts of the FSO technology, its principles of operation, advantages, and then the limitations. Further, the exact security threats that FSO systems are prone to are presented and organized into physical, network, and application-level threats. This paper gives an in-depth review of the current security mechanisms applied in FSO, such as encryption techniques and physical layer defenses. However, this paper discusses emerging trends and technologies holding tremendous promise for enhancing FSO security. For instance, a probable result of integrating artificial intelligence and machine learning and utilizing mechanisms like Quantum Key Distribution into FSO systems would be the adaptation of mechanisms for security that are able to detect and mitigate threats in real time. It also provides some potential areas for future research, like developing standardized security frameworks specifically for FSO communication and exploring hybrid systems bringing together advantages of FSO and RF technologies [16]. The main goals of this review is to analyze the key security issues affecting FSO communications and examine the various existing mitigation techniques and measure their efficacy. Discuss new trends and technologies that would help improve the security of the FSO network. Identify current gaps in the area of research and propose future research directions.

The rest of this paper is organized as follows. Section 2 gives the basic principles of FSO communication, such as the principles of transmission, advantages, and challenges. Section 3 highlights the exact security threats facing FSO systems, which are consequently structured into threat models and attack vectors. Section 4 is devoted to the review of existing security mechanisms and the possibility of their application in different contexts. The new trends and state-of-the-art solutions in FSO security are presented in Section 5, covering new approaches and future lines of research. Gaps in the current body of research are identified in Section 8, pointing to areas where more work is required. Finally, Section 6 presents the conclusion of the paper, with key takeaways and implications for ongoing research in this area. This paper aims to serve as a comprehensive resource for researchers and practitioners in the field of optical communication, offering insights into the current state of FSO security and guiding future efforts to develop more robust and resilient systems.

## II. BASICS OF FSO COMMUNICATION

FSO communication is a technique of wireless communication that conveys the transferred data by beams of light moving through the atmosphere. In contrast to traditional fiber optic communications, which depend on guided media, FSO deploys unguided channels. Hence, it becomes a perfect solution in those cases where physical cabling is not possible or very expensive. The following section provides insights into basic components, operational principles, modulation techniques, applications and challenges of FSO communication to help in fully understanding this technology [17, 18].

### *A. FSO Systems*

The basic elements of an FSO communication system are mainly three: the transmitter, the channel, and the receiver. For the FSO Transmitter, the signal or data generator generates the original data in the transmitter section of a FSO communication system, most often error-corrective coding, such as LDPC, for reliable transmission. Basically, a signal undergoes data processing, which includes encoding, and modulations. Finally, the signal is converted into an optical signal via the Driver and Optical Source (Laser) and then amplified optically, thus preparing it for free space transmission through the transmitting antenna. In the FSO system a laser diode generates the optical signal. These diodes find applications in long-distance, high-data-rate kinds of applications because of their narrow beam divergence, high output power, and ability to retain focus. LEDs are less powerful and, therefore, more suitable for short-range applications such as VLC [19], where a wide divergence angle is more important than the range. The data to be transmitted can be encoded on the optical signal using a number of modulation techniques, which are detailed later on [20].

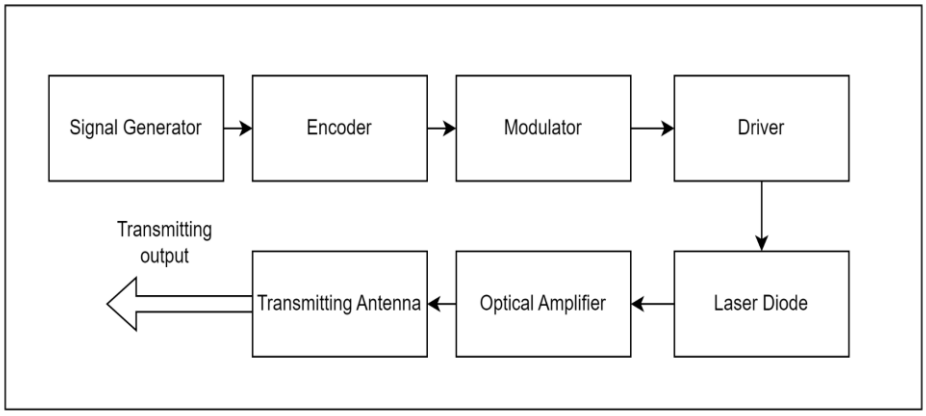


**Fig 1: Transmitter for FSO Communication System**

In Free Space Optical (FSO) Communication, the channel is an open medium of air through which optical signals, normally laser beams, propagate. In contrast with wired communications and their fiber optics counterpart, the FSO channel is affected by atmospheric turbulence, fog, rain, and obstacles that may dissipate or interrupt the signal. FSO channels are highly directional and require a free line of sight between transmitter and receiver. The received optical signal is detected by the Photo Detectors, such as PIN diodes or APDs, and in the receiver of a FSO Communication system, it changes the optical signal into an electrical one. Most of the time, APD types are preferred because of their high sensitivity, which is crucial to detect weak optical signals in situations with long-distance communications. The weak current, after processing through a transimpedance amplifier, results in a usable voltage. Noise reduction and further amplification of the signal are applied for its clearer reception. Later, at the post-processing stage, the signal is first demodulated, then filtered for noise removal, and combined in case of splitting during transmission. Lastly, the Decoder, like a LDPC error correction block, corrects any errors and produces clean, accurate output data [20].

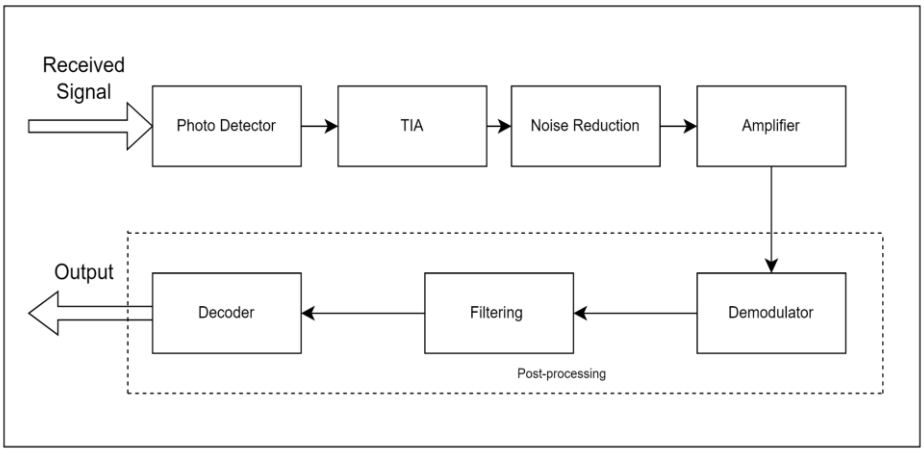


**Fig 2: Receiver for FSO Communication System**

A set of optical components inside both transmitter and receiver ensure proper focusing and alignment of the light beam. FSO systems include various optical components including lenses, collimators, and beam expander to create a stable, directed optical link. Lenses are used to focus light in a very narrow beam that reduces the divergence of the beam, hence reducing signal loss with distance. Collimators will maintain the parallel structure of the light beam during its travel to enhance further the integrity of the signal. Some systems use beam expanders to reduce divergence of the beam increasing the coverage area of the optical signal. Acquisition, Pointing and Tracking (ATP) Systems are used in FSO communication as the transmitter has to be continuously aligned with the receiver because of the very directional nature of the optical beam. A small misalignment on the order of milliradians results in significant signal attenuation or even loss of communication. APT systems keep the optical beam aligned in the line of sight amid dynamic scenes with relative movement between the transmitter and receiver. Alignment by such systems is continuously monitored and allows adjustments in real time to ensure stable communication [21, 22].

### *B. FSO Operational Principles*

FSO works on the principle of line-of-sight transmission, whereby modulated light is directly transmitted from the transmitter to the receiver. LoS transmission is ensured by the careful alignment of the optical components so that the light beam is kept focused and directed over the distance of interest. The wavelength of light used in any given FSO system makes all the difference. Most FSO systems lie within the infrared portion of the spectrum; normally, they range between 780 nm - 1600 nm. This range is chosen due to the positive propagation characteristics within the atmosphere, which include low absorption and scattering by atmospheric particles. In particular, wavelengths around 1550 nm are used because they correspond to better laser eye safety, reduced solar background radiation, they can penetrate fog at longer distances and they have somewhat better receiver sensitivity for PIN detectors compared to 800 nm. For VLC systems the range is from 400 to 700 nm. Visible spectrum is, however, more prone to interference from other ambient light sources like sunlight or artificial lighting, hence requiring robust filtering and signal processing techniques [23,24].

Efficient data transmission in FSO communication relies greatly on the modulation techniques used to encode information into the light beam. Common modulation schemes include [25, 26] :

**1.** On-Off Keying (OOK): OOK is the simplest form of modulation techniques used in FSO communication. The on and off of light from the source represent data. Light 'on' corresponds to binary "1" and 'off' corresponds to binary "0." Although this process is quite simple, it is power-intensive and prone to noise; therefore, it is not that suitable for line-of-sight applications at long ranges or high speeds.

**2.** Quadrature Amplitude Modulation (QAM): QAM links both amplitude and phase modulation together, and therefore it can transmit more than one bit per symbol. This increase in the modulation technique brings about anincreased data rate but requires sophisticated designs at the receiver and is more susceptible to noise and interference in poor atmospheric conditions.

**3.** Pulse Position Modulation (PPM): In PPM, data is encoded by varying the position of optical pulses within a fixed frame. This scheme has better noise immunity compared to OOK and is power-efficient; thus, it is suitable for applications that consider the aspect of energy conservation. Perfect timing synchronization between the transmitter and the receiver is required for PPM, which can complicate the design of the whole system.

**4.** Differential Phase Shift Keying (DPSK): DPSK is a method of modulation that encodes a signal based on the phase difference between two successive pulses. Due to this fact, it is highly resistant to phase noise and can, therefore, be used in high-speed FSO links where signal integrity is important.

**5.** Orbital Angular Momentum (OAM): In OAM a phase structure of the optical beam is used for encoding by twisting its phase front, with each OAM mode acting as a separate data channel. As the FSO systems allow multiple data channels to be transmitted at the same time on different modes of OAM, it enhances the capacity and makes it suitable for high-capacity and high-speed communication [27-30].

**6.** Color Shift Keying (CSK): CSK does the modulation of data depending on the color or wavelength of the optical signal. In CSK, a different color shift will correspond to a different value of data, and it enables multiple bits to be transmitted per signal pulse. This technique has the possibility of improving data rates and spectral efficiency, which would, however, depend on precise control of the wavelength and stability of the optical components [31-33].

Beam characteristics and alignment, directionality and focus are among the key factors which affect the performance of FSO communication through the optical beam. Due to the extreme narrow divergence of laser beams, the signal remains

pencil-like over long distances with minimum power loss and increased received signal strength. This high directionality makes the system more vulnerable to misalignment. Even slight shifts in alignment may result in the beam missing the receiver, which may then cause large degradation in signal levels or communication failure [20],[21]. This is further exacerbated in the scenarios where there is relative movement between the transmitter and receiver, like in satellite communication or mobile platform applications. For this very reason, FSO systems are equipped with PATs that continuously track the beam alignment to compensate for any kind of disturbances or movements that can affect the signal path.

### *C. Challenges in FSO Communication*

Although FSO communication has several advantages, it suffers from a number of challenges affecting its reliability and performance. These originate from the very open-air nature of the transmission medium that exposes the optical signal to various environmental and operational factors [34].

**1. Atmospheric Absorption and Scattering**:

The medium through which FSO technology transmits the signals is free space – air, atmosphere, deep space – that means the signal does not have the protection of physical medium and has to endure atmospheric absorption and scattering. The presence of water molecules, carbon dioxide, and ozone in the atmosphere can absorb light, leading to signal attenuation. Scattering occurs due to particles like aerosols or dust, which can divert the light path. Weather conditions like rain, fog, snowfall, or dust negatively impact the line of sight of an FSO system, resulting in severe attenuation and scattering of light.

Droplets of rain can absorb and scatter the optical signal, bringing down its power at the receiver. The amount of attenuation all depends on the droplet size and density and the used wavelength. Fog is one of the most critical challenges in FSO communication. Due to the high density of water droplets, light travels in every direction and hence faces huge attenuation. The link can even completely drop in extreme dense fog conditions. Snowflakes and dust particles alike scatter and absorb, hence resulting in effects to the signal strength and quality. The impact varies with particle size and concentration in the air.

**2. Atmospheric Turbulence:**

Atmospheric turbulence, caused by temperature and pressure changes, is responsible for random variations in the refractive index of the air over the transmission path. This turbulence leads to a few challenges such as Beam Wander, Scintillation and Phase Front Distortion. In **beam wander** the optical beam may be deviated from its desired path due to turbulence, which causes momentary misalignment and results in signal loss. Turbulence induces fast changes in the refractive index and, hence, in the intensity of the received signal, which is called scintillation. In this respect, **scintillation** can cause fading of the signal, leading to a raised BER and degraded communication quality. The variation of the refractive index can cause **phase front distortion** of the optical beam, leading to demodulation error of the signal and hence decreasing the overall reliability of the system. The impact of atmospheric disturbances imposes a limit on the maximum link distance realizable within an FSO system. It can have reduced reliability with increasing distances, especially in bad weather conditions [35-37].

**3. Beam Misalignment Problems**

One of the most challenging problems to be overcome in FSO communication is the proper alignment between transmitter and receiver. This misalignment could result from wind, building vibrations, or simply the relative motion of the communicating platforms. In applications like satellite communication or mobile networks, where one end or both are in motion, dynamic realignment is required. This is possible through the inclusion of more advanced Aligning, Tracking and Pointing (ATP) systems that track dynamically the beam direction variations and hence ensure stable communication. Various studies have presented adaptive control strategies, low-power beam mitigation techniques, and fuzzy logic controllers that improve alignment and overall performance in FSO systems. An essential part of FSO communication systems is beam steering techniques that ensure that the transmitter and receiver remain aligned, particularly when operated in the presence of atmospheric turbulence and beam wander. Closed-loop feedback systems and beam wandering compensation techniques improve the stability of optical links to adjust dynamically the direction of their beams [38-41].

**4. Background Noise and LoS Obstructions**:

A problem is that background light from sources such as the sun, street, and indoor lights introduces noise into the system in VLC applications. Robust filtering techniques are needed to separate the desired signal from the ambient noise and provide consistency and security for the communication. Since communication using FSO is LoS communication, any physical obstruction, such as buildings, trees, or sometimes even birds, will partially or totally block the beam path, thus blocking signal transmission for temporary periods. Proper system design with considerations for parameters like beam divergence, transmitter power, and receiver field of view can stem this issue now and again.

### *D. Applications of FSO Communication*

FSO communication finds applications in very broad fields. This has been driven by its ability to offer high speed, security, and flexibility of data transmission in scenarios where traditional methods of communication are limited or impractical.[5, 6].

**1. Optical Space Communication:**

FSO technology finds increasing applications in satellite communication, like setting up high-speed data links between satellites (inter-satellite links) and between satellites and ground stations (downlinks and uplinks). High data rates and low latency make it immune to RF interference; thus, FSO is the best option for deep-space missions and links that interconnect LEO satellites. NASA's Deep Space Optical Communication (DSOC) Project will demonstrate high-speed optical communication from deep space using a specialized laser transceiver on the Psyche mission spacecraft, aiming to enhance future space communication [42].

**2. Urban Wireless Networks and Last-Mile Access**:

In the populous centers of towns, laying fiber optic cables for high-speed Internet access is at times squarely discouraged by space constraints and high costs involved. FSO provides an effective, low-cost, easily deployable alternative to establish last-mile connectivity without the need for extensive cabling. This is done for service providers who aim to offer high-capacity Internet access by interlinking buildings, towers, and other infrastructure using FSO links [43-46].

**3. 5G Backhaul and Beyond**:

With the expansion of 5G networks, there is an increase in demand for high-capacity backhaul links. For this purpose, FSO is able to offer an appropriate solution by delivering several gigabit-level data rates with low latency. In areas where deploying fiber is not feasible, FSO can bridge the gap to ensure seamless communication between network nodes [47-49].

**4. Disaster Recovery and Emergency Communication**:

FSO systems can quickly be set up to restore communication in disaster situations that may damage or render unavailable existing communications infrastructure. This quick setup, with the independence from pre-existing infrastructure, provides a technology of great benefit to many emergency response operations [50, 51].

**5. Military and Government Communications** :

The security and resilience of FSO communication against jamming and interception make it one of the most preferred options for military and government applications. FSO links are used to build secure data transfers, especially in sensitive operations, where information is highly critical and intended to be kept away from possible opponents [52-54].

The basics of communication through FSO describe its potential and, at the same time, the problems that must be tackled. High data rates, used unlicensed spectrum, and ease of deployment combine to place the FSO as a resourceful tool for current communication needs. However, overcoming the limitations of atmospheric conditions, alignment requirements, and interference is crucial in achieving reliable and secure FSO links. Continued evolution of technology and ongoing research point toward mitigating these challenges through advanced modulation techniques, adaptive optics, and intelligent system designs that will ensure further expansion of FSO communication into wide-ranging applications.

## III. SECURITY CHALLENGES IN FSO COMMUNICATION

FSO communication systems include unique security issues based on an unguided light beam dependency in open air for transmission. Although the intrinsic properties of FSO, such as directionality and narrow beam width, give some security, still they could not hold against various threats like eavesdropping, jamming, or even physical layer attacks. This part further provides insight into the security challenges through discussing some key threats and vulnerabilities, attack techniques, and current countermeasures.

### *A. Eavesdropping and Interception*

The major vulnerability in FSO communication is the exposure of the beams carrying the data through the atmosphere and then to the receiver. As opposed to fiber optic systems, where the light signal is confined within a cable, FSO systems are built on unguided channels and are quite prone to interception. The exposure opens up the possibility for unauthorized entities to eavesdrop on the communication by placing a receiver in the line-of-sight (LoS) path of the optical beam. Eavesdropping involves no physical tampering and is hence pretty hard to detect, especially when the attackers are equipped with sophisticated techniques of capturing the signal without being noticed. Because the beams transmitted in FSO are narrow and very directional, this actually provides some inherent resistance against interception. Successful eavesdropping requires the interceptor to align his receiver very precisely along the optical path, which can be difficult to do. However, if the beam is slightly divergent because of atmospheric perturbations or misalignment, these can be exploited by enemies for gaining access to the signal. In cities or other areas of high-density reflection, this sort of scattering or deflection of light in urban scenes will, however, give access to data for attackers, hence will not require direct LoS.

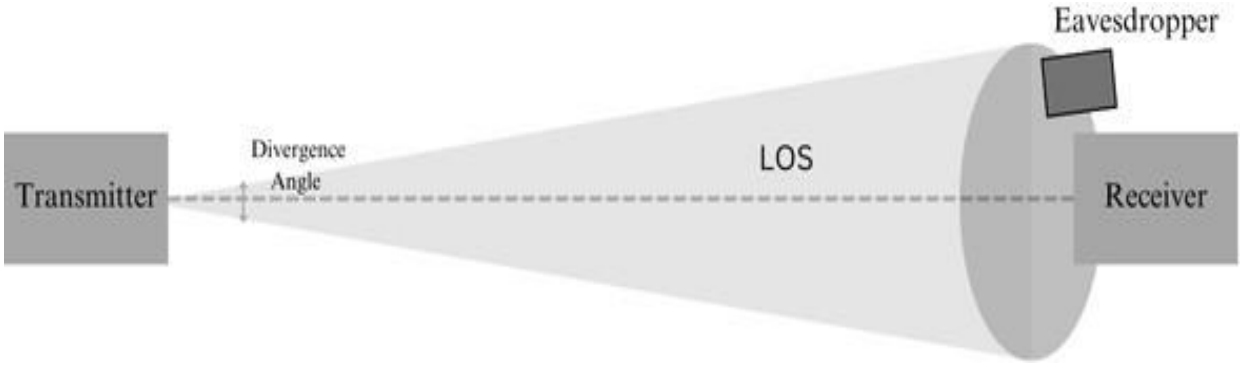


**Fig 3: LoS Interception: Eavesdropper near Receiver**

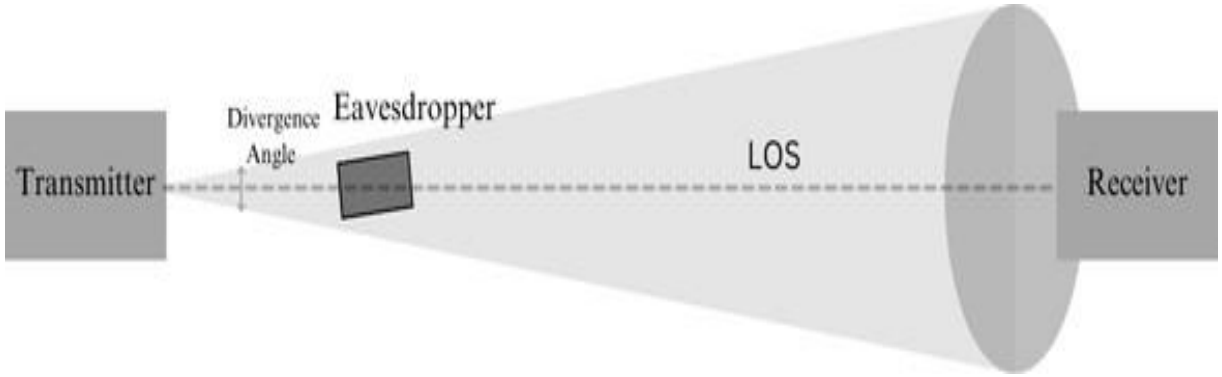


**Fig 4: LoS Interception: Eavesdropper near Transmitter**

FSO is vulnerable to interception by the enemies through several techniques: The simplest ones rely on a receiver located in the path of the beam, which is in the direct line of sight. When the attacker carefully adjusts their receiver corresponding to the optical link, they can capture and decode the transmitted data [55]. Alternatively, more sophisticated methods use beam splitting, where modulated light is deflected to a small fraction of the main beam through optical devices (as shown in Fig 3 and Fig 4). This may be performed without altering the main signal in a significant manner, thus making it very difficult to detect the interception. The second way is through optical tapping, by means of which a small part of the transmitted optical beam is sucked out through specialized equipment that is designed to extract light from the main transmission with little perturbation (as shown in Fig 5) [56]. This form of interception becomes particularly hazardous as it gets to be very subtle and thus allows the capture of data continuously over long periods of time. Moreover, attackers may be able to leverage the atmospheric scattering by using advanced sensors trying to capture the stray light associated with the primary beam. The light captured is weaker, but it is possible to recover the data with meaningful strength using modern amplification and signal processing methods. That method will become a grave threat to communications confidentiality.

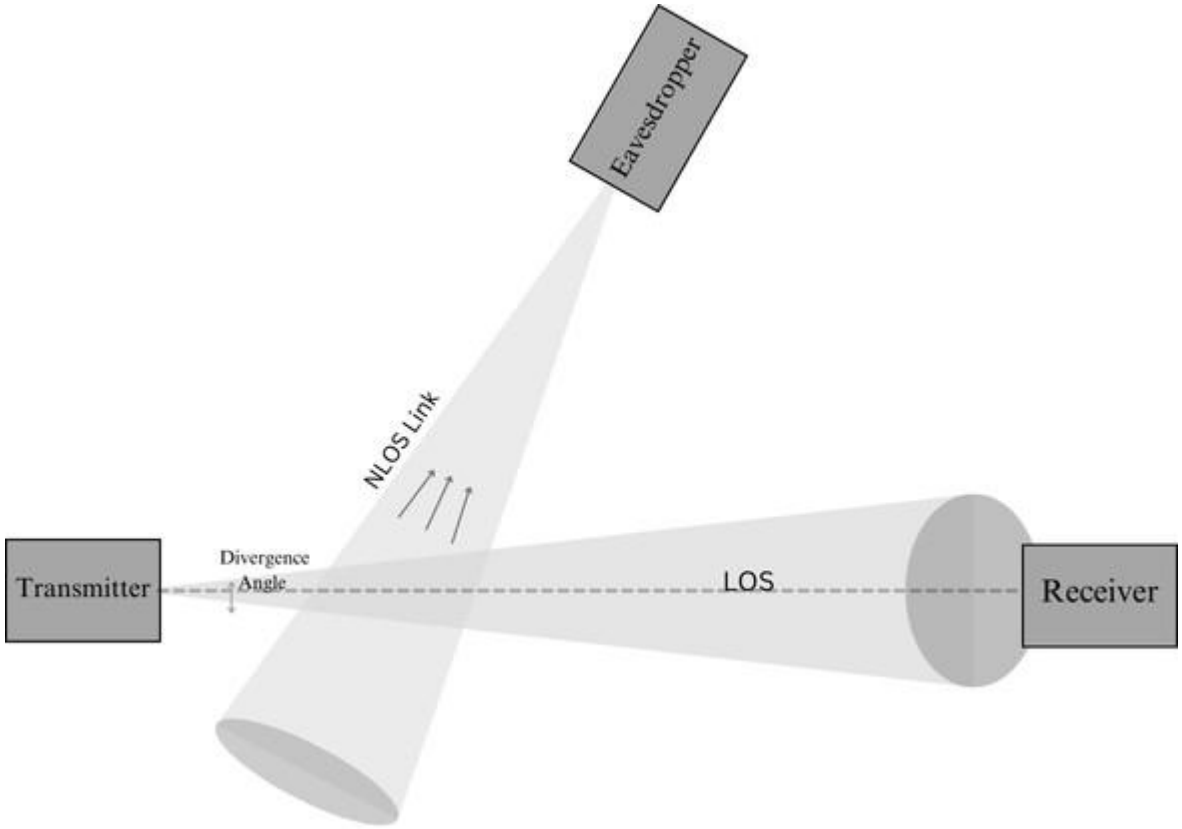


**Fig. 5: Non-Line-of-Sight (NLoS) Interception**

Several countermeasure strategies can be adopted to counter these eavesdropping techniques:. One is that, by decreasing the beam width and power dynamically, it reduces chances of interception by an unauthorized receiver. By maintaining the optical beam focus and alignment tightly, there is very little chance of stray light that can fall in the unintended receiver. This method has its own challenges. Narrower beams would require more alignment preciseness and increase the chances of misalignment that could arise because of a small fluctuation of either the source or the destination. This misalignment can be more frequent in long-distance or dynamic environments. This is why several beam position tracking are used as corrective measures [57, 58]. Another way would be to make the transmitted signal from a Gaussian beam together with a low powered vortex beam. And select the detectors with the maximum received power for the particular signal, depending on the spatial distribution probability of the signal beam [59, 60]. Another important point in ensuring that communication using FSO cannot be eavesdropped upon is the encryption of the data being sent. While an attacker can intercept the signal, the data itself will not be readable without the correct decryption keys. Although it is a very effective measure, it adds computational overhead and thus requires efficient strategies for key management, especially in the case of large or rapidly changing FSO networks. In paper [61], spontaneous emission light sources are used. The optical delays between transmitter and receiver are used to protect the signal from interception. The receiver can receive the signal only when the delay length and the pre-shared keys [62].

Deep Learning or Machine Learning can be also used to detect users and interlopers among them. A paper explores using convolutional neural networks (CNNs) for eavesdropper detection in free-space optical (FSO) communication systems with ON-OFF keying (OOK). The CNN outperforms traditional methods like SVMs, showing high detection accuracy under varying eavesdropping conditions and signal-to-noise ratios (SNR) [63]. An unsupervised machine learning approach to real-time identification of the number of active transmitting users in multi-point free-space optical communication systems that only requires amplitude information with clustering algorithms, using a histogram peak detection method along with a weighted clustering analysis in case the power levels of the users are very close. Experimental results show accurate estimation of the users even in very severe atmospheric turbulence conditions. Future work will be directed toward determining the minimum sample size that can guarantee effective detection [63]. In the paper [64], the performance of EST in relay-assisted FSO systems under various weather conditions and in the presence of eavesdroppers is evaluated. The study contributed by proving that relay-assisted FSO systems guarantee better security and reliability in harsh environments like disaster recovery scenarios [64]. Another paper evaluates the secrecy performance of FSO systems with respect to misalignments, eavesdropper location, and atmospheric turbulence using

Log-Normal and Gamma-Gamma models. New metrics are proposed for quantifying security: outage secrecy capacity and strictly positive secrecy capacity. Results indicate that proximity of the eavesdropper and misalignment errors grossly reduce secrecy. The study provides insight into how to optimize secure FSO systems under realistic conditions [65].

The paper [66], compares the secrecy performance of RF and FSO links in the mixed RF-FSO relay network setting under eavesdropping attacks. While the links are much more secure in FSO than in RF due to their directional nature, actual effectiveness could be compromised due to adverse weather. The study thus puts forward optimal relay positioning and environment considerations in enhancing security in hybrid communication systems [66]. [67] discusses the feasibility of performing an intercept-resend attack on free-space quantum key distribution systems undergoing atmospheric turbulence with a phase-only SLM. The findings are that turbulence effectively mangles Eve's ability to accurately intercept and resend signals; however, with adaptive optics such as tip-tilt correction, it is possible to have successful attacks in conditions of moderate turbulence. In this study, it is shown that a threshold beyond which these attacks are not feasible does exist, hence giving insight into QKD security in real conditions [67].

Despite such counter-measures, FSO systems still suffer from certain advanced-design attacks. Power adjustments in a dynamic manner can hinder performance in different atmospheric conditions, whereas certain encryption techniques may fail to offer complete resistance to side-channel attacks, which are threats that exploit physical phenomena, not breaking encryption algorithms.

### *B. Jamming and Denial of Service (DoS) Attacks*

One of the greatest security threats against FSO communication systems is jamming. By introducing a high-powered signal or noise into the communication channel, the attacker can disrupt or block the legitimate transmission of data, leading to a Denial-of-Service attack. Because FSO systems rely on a narrow path of transmission and reception, they are quite vulnerable to focused jamming efforts. An attacker can simply beam an interfering optical ray on the receiver, thus making the legitimate signal insignificant or breaking down communication [68]. Jammers fall into one of the two categories: a persistent jammer or a random jammer. A persistent jammer keeps on transmitting the jamming signal regardless of the data it is carrying through the network. It reserves random bits introduced into the channel used for communication and transmits on one channel until the random bits are completely used up without even changing frequencies. On the other hand, a random jammer focuses on energy conservation, switching between idle and jamming phases. It remains inactive for some time before activation to jam the beam. Also, these periods can be fixed or their length can be controlled both in standard FSO systems mitigating laser level safety issues and also, the jammers can switch on and off irrespectively of eye safety measures [69].

Such attacks can have a very draining effect on FSO communication, especially in time-critical or mission-critical applications. So, if the jamming attack is successful, it might go as far as totally losing communications, degraded performance, or increased error rates, thereby making the link very unreliable. This could easily result in disastrously bad news for military or rescue missions in terms of failed missions or compromised safety. Various countermeasures could be applied to reduce the conduct of jamming attacks. An attempted interference cannot be made to be coherent for long enough if the system changes frequencies quickly, in the technique referred to as frequency hopping. Alteration in the optical beam characteristics and thus minimizing the jamming signal could also be performed by beam shaping and adaptive optics. Polarization and filtering mechanisms could further be enforced to reject the unwarranted signals, thus adding to the system's robustness against interference.

The performance of the system can still be seriously degraded by sophisticated jammers set on their mission, particularly since the FSO link is already susceptible to environmental problems. Several papers discuss the effects of Jamming on the FSO communication system and its mitigation techniques. [70] discusses the effect of relay jamming on a decode-and-forward cooperative FSO system by focusing on performance degradation due to a mixture of additive Gaussian and exponentially distributed noise. In this paper, it has been shown that a threshold-based detector can achieve almost the same performance as a maximum-likelihood detector under high jamming power, and a closed-form BER expression has been derived. Numerical results demonstrate substantial performance losses, particularly under severe jamming and low pointing errors in the jamming link [70]. [71] uses an optimization technique for maximizing the FSO power emitted to the directed receiver and minimizing the power leakage into the main lobe to minimize interference and eavesdropping. The stochastic evolutionary algorithm suppresses over 10 dB near the receiver with sufficiently good signal quality. They concluded that smaller spacing was needed between consecutive suppression points, and high transmitting power near the receiver, and aperture fill factors affect system performance, smaller fill factors imply higher chances of interference [71].

In the following papers the jamming impact on SISO/MIMO FSO Systems are studied particularly. In [72], the authors investigate the performance of jamming over atmospheric turbulence fading channels with negative exponential and Gamma-Gamma models for SISO FSO systems. A theoretical framework is set up where the average bit error rate under jamming is analyzed, unveiling how jamming results in non-Gaussian noise degradation. The results show that a 2

× 1 FSO system is more robust to mitigate jamming effects than SISO, and as the jamming intensity is lowered or more transmit apertures are added, better performance is achieved [72]. [73] evaluates the jamming effect in SISO/MISO FSO systems over Gamma-Gamma fading channels with pointing error effects and derives the BER performance in closed form under jamming. The results show that, in the case of high additive GG noise, the BER performance for SISO systems is not good. From numerical analysis the authors inferred that in low signal-to-jamming ratio scenarios, the always-on jammer induces significantly more errors than in high SJR scenarios, where the low-probability jammer becomes very harmful. The study concludes by stating that a MISO FSO system performs way above a SISO system in mitigating jamming effects [73].

Many Machine Learning techniques have also emerged to mitigate effects of jamming on FSO Communication. This paper presents two machine learning-based algorithms to classify the structured light modes. And it also assesses SJR in FSO communication under jamming. In the first part, a classification algorithm is implemented, where the SVM and histograms of oriented gradients are utilized to identify light modes as 8-ary LG and 16-ary HG. The second is the ANN model, used to predict SJR values within -5 dB to 3 dB. Results are taken to be satisfactory in the sense that classification accuracy is improved and ML models are able to determine modes besides estimating SJR in difficult jamming scenarios [74]. [75] discusses the applicability of machine learning to identify structured light patterns using CNNs in FSO systems under jamming attacks. In particular, it has been demonstrated that these CNNs realize very high accuracy in recognizing modulation schemes and the determination of a jammer direction where standard LG modes are shown to be very susceptible to jamming in low signal-to-jammer ratios [75]. [76] compares various machine learning techniques, including ANN and support vector machines, among others, for their efficacy in detecting power jamming attacks in optical networks. In this respect, this paper has concluded that ANNs show the highest accuracy in the identification of out-of-band jamming. The authors further propose a resource reallocation scheme based on detection accuracy to mitigate these attacks, where the probability of successful jamming is decreased with the enhanced effectiveness of network security [76].

The [77] considers the issues of jamming attacks on 6G networks, focusing on extreme bandwidth communication technologies like millimeter waves, terahertz, free-space optical, and visible light communications. An all-rounded review is provided on jamming types, anti-jamming techniques, and parameters that could affect susceptibilityto jamming in such technologies. In this regard, the paper puts a premium on continuous research toward robust, jamming-resistant solutions that can provide secure and dependable 6G networks [77]. The researchers have gone one step ahead from finding solutions for jamming to utilizing jamming to disrupt potential eavesdroppers. This concept is known as Friendly Jamming, in which the friendly nodes intentionally inject jamming signals to potential eavesdroppers, effectively stopping them from intercepting the legitimate communication between authorized networks. The legitimate receiver is either unaffected by jamming because of specific design measures or being able to filter out the jamming patterns by knowing them in advance. In [78], a random dual-node cooperative jamming scheme was proposed for secure transmission in line-of-sight wireless communication networks that involve a sender, receiver, a few helpers, and a passive eavesdropper. The location of the eavesdropper is unknown to the helpers, who simply try to perform uniform jamming in every direction except towards the intended legitimate receiver. Simulation results indicate that the random jamming scheme performs far better than traditional cooperative jamming in terms of outage probability, for lower system costs and very small channel information sharing among nodes [78].

### *C. Physical Layer Security*

The optical beam naturally diverges in FSO communication as it propagates over long distances. Divergence enhances this risk by increasing the footprint of the beam, which can potentially expose the signal to eavesdroppers. Adding to this is misalignment, which can be affected by environmental conditions—such as wind, vibration, and/or platform movement in dynamic scenarios—thereby further increasing this risk. Major performance degradation can occur even from very small misalignments because the beam may not completely or partially strike the receiver. For mobile platforms, like drones or moving vehicles, perfect beam alignment is always difficult to ensure. Here, the system is not only susceptible to interception but also to jamming since misaligned beams spread into parts of the space where attackers can more easily target for jamming [79]. This requires advanced mechanisms of alignment and real-time tracking systems [80]; however,

this raises the complexity and cost of a system. Atmospheric turbulence causes random fluctuations in the refractive index of air, which, in turn, induces beam wander, scintillation, and phase front distortions. These effects can lead to degradation of the optical wavefront at a receiver and an increase in the bit error rate. Additionally, optical beams are scattered by turbulence, giving rise to secondary paths off the main line-of-sight link. Information on these scatter signals can be used by an eavesdropper to collect enough light to recover the transmitted data. Scattering is especially strong in urban settings or regions of high dust and aerosol concentrations because these particles strengthen scattering. Even when the primary beam does not reveal any useful intelligence to the enemy, the scattered components might be sufficiently intense to be useful from afar to an enemy, who may be anywhere except at the intended receiver, thus rendering the system non-secure. For example, multipath interference through many reflected buildings, vehicles, or general surfaces in a densely populated area, can cause the creation of numerous distinct signal paths that might result in delayed signals and data corruption. Attackers can magnify the effect by developing reflective surfaces within the transmission environment, thereby deliberately adding interference to distort communication quality. This type of attack can be deployed most effectively in conditions that make it difficult to achieve a clear line-of-sight, such as in metropolitan areas with complicated infrastructures.

FSO systems need to have strong filtering and compensation strategies for integration into them to reduce multipath. However, unlike the previous means, those are often very resource-intensive, and in some environmental cluttered or reflective environments, even the effect cannot be completely mitigated. [14] explores the potential of Optical Wireless Communication and its advantages over RF networks. The authors have very succinctly conducted a survey on physical layer security in optical wireless communication (OWC) which includes both FSO Communication and Visible Light Communication (VLC) [14]. [81] presents an overview of progress in physical-layer security for free-space optical communication systems and their advantages compared to traditional radio-frequency networks. FSO systems can provide better security compared with RF-based systems due to their very narrow optical beam and line-of-sight components, making them less prone to eavesdropping [81]. On the other hand, FSO networks can suffer from atmospheric turbulence and bad weather conditions that will degrade the system performance. It details some of the FSO systems: SISO FSO links, mixed FSO-RF, and hybrid FSO/RF systems, showing how various factors, including input signaling, atmospheric conditions, and eavesdropper location, affect secrecy performance. The paper also highlights open research challenges that can be aimed at optimizing security in FSO systems.

The following studies showcase scenarios in which the FSO Communication system is vulnerable in relation to Physical Layer Security. [56] provides an overview of the physical layer security behind free-space optical communications, showing two scenarios: An eavesdropper near the transmitter in an EnA scenario, which easily compromises the communication, which slightly extracts power from the laser beam, especially when legitimate transmitter receiver pairs are far apart. Secondly, an eavesdropper near the receiver EnB while comparatively less effective, but the random fluctuations of the signal can easily introduce a security risk. This means that new design considerations concerning FSO systems are necessary, and it creates opportunities for further research in the development of advanced eavesdropping techniques [56]. [55] discusses the security risks that free-space optical communication systems may have in the presence of a possible eavesdropper outside the laser beam, connected through a non-line-of-sight (NLoS) scattering channel. The results obtained show that there are minimal security risks when the visibility is high but increase drastically in scenarios of low visibility. It also demonstrates a 2-D distribution of secrecy capacity due to location changes by the eavesdropper and realizes that the performance of secure transmission with this system is highly dependent on background radiation and the required rate of transmission under strong turbulence [55].

[82] discusses the generalization of Wyner's wiretap channel model in free-space optical communication, concentrating on impact due to the eavesdropper attack due to optical beam-splitting. The research showed that even though PLS can be compromised, positive secrecy capacity can still be achieved by exploiting the noisy and degraded conditions of the eavesdropper channel. Experiments with Bessel–Gaussian beams have shown that the BER of an eavesdropper was always higher compared to that at the intended receiver, hence proving a security advantage. This approach does not provide unconditional security, though it could be achievable in the future by incorporating quantum key distribution [82].

There are several studies conducted on improving Physical Layer Security in FSO Communication which will be discussed in the next section.

### *D. Atmospheric Effects on Security*

Severe weather conditions such as fog, rain, and snow result in intense attenuation of the signal level and therefore reduction of the communication range for the FSO communication systems. In bad weather, the optical beam might

scatter, be absorbed, or reflected by atmospheric particles, thus causing signal loss or degradation. With these factors, the conditions do not only affect the link in terms of reliability but can create an opportunity for a malicious adversary to eavesdrop on or jam the communication during such a state of operation at reduced capacity. For example, under very dense fog, the attenuation can be quite high and the signal may be considered to be practically untraceable, dueto which communication breaks down literally. This is very risky with respect to security for military operations or for the financial data transfer, in which cases it is often made use of by the attackers for using the weakened links for injecting noise, intercepting data, or making use of denial of service attacks.

Based on meteorological parameters, this paper [83] intends to develop and validate mathematical models predicting the optical attenuation with a high accuracy across different seasons, using linear regression and ANOVA tools in FSO communication [82, 96]. In the paper [84], a study has been presented that shows the impact of atmospheric turbulence on the BER of Wireless Digital Laser Communication Links (WDLCL). The design of the low cost FPGA-based Bit Error Rate Tester has also been described and analyzed its behavior under different conditions [83]. A model for predicting atmospheric turbulence strength in Free-Space Optical Communication FSOC systems is developed using meteorological data and validated to achieve high accuracy over various seasons, while showing an average prediction error as $2.3\times10-13$ $m-2/3$ [85, 86]. A paper presents an FPGA-based closed-loop control system using a position sensing detector (PSD) and stochastic parallel gradient descent algorithm (SPGDA) to enhance laser beam alignment, tracking, and positioning in FSO Communication [87]. The paper [88] presents a Terrestrial Free Space Point-to-Point Laser Communication (TFSPPLC) system using adaptive optics and FPGA-based fuzzy logic control to mitigate atmospheric distortions, enhance signal alignment, and analyze the experimental data in real-time over a 500m link [88]. [89] demonstrates the design and implementation of an adaptive fuzzy logic controller in FPGA with the aim of reducing the impacts of atmospheric effects on laser beam alignment, tracking, and positioning in FSO Communication systems. Another paper describes the development of advanced Electronic Warfare (EW) systems which integrate Active Electronically Scanned Array (AESA) technology with miniaturized planar arrays and Field Programmable Gate Arrays (FPGA) for steering and controlling the beam in the 5-18 GHz frequency range [90]. In [91] , two controllers—Taguchi's Response Surface Model (RSM) and Artificial Neural Network (ANN)—are compared while stabilizing the beam wander in Free Space Optical links, both implemented in FPGA, and tested over a 0.5 km horizontal range [91,92]. Another paper details a beam steering technique using a Position Sensitive Detector (PSD) and a low-cost Fast Steering Mirror (FSM) to improve Free-Space Optical Communication (FSOC) and FSOC to Single Mode Fiber (SMF) coupling, with experimental validation of the system's performance [93]. In [94], based on the functionality of the designed FPGA controller, experimental testing of the efficiency of the Taguchi and ANN controllers in FPGA for stabilizing the focus of the laser beam and limiting the power loss in free space optical links is presented [94]. The paper [95], provided a high-accuracy model for the prediction of optical attenuation in Free Space Optical Communication systems based on parameters of meteorology, whose R 2 value was demonstrated at 98.76%, and average RMSE over a year is 0.043 dB/km [95].

A few studies explore the effect of atmosphere on FSO systems with different types of modulation schemes. [97] investigates the performance of bit error rate (BER) for free-space optical (FSO) communication systems with strong atmospheric turbulence with different schemes of modulation including on-off keying (OOK), binary phase-shift keying (BPSK), differential phase-shift keying (DPSK), quadrature phase-shift keying (QPSK), and 8-phase shift keying (8-PSK) for link distances of 500, 1000, 1500, and 2000 meters. In this scenario, the model of the gamma-gamma distribution is used to describe the probability density function of the received irradiance. Results indicate that the performance of BPSK in both BER and power compensation is the best among these three schemes and that of OOK is the worst. For the FSO system with moderate-to-strong turbulence channels, using BPSK is recommended as a modulation scheme, and using OOK is discouraged [97]. [98] examines the impact of the weather on FSO systems with Wavelength Division Multiplex used to optimize the quality of data transmission. FSO systems highly depend on the weather conditions, whereby haze and rain provide a considerable reduction of signal power. The analysis reveals the wavelength of 1550 nm to be less influenced by atmospheric attenuation, shorter distance of the link between transmitter and receiver in order to provide high system performance. The study proposes an FSO system to have a data rate of 2.5 Gbps, with a wavelength of 1550 nm, corresponding to an achievement of a link range up to 150 km in clear weather with a BER at 10-9. Simulations show that, while clear weather supports longer distances, rain and haze are the two worst ones that hit performance very hard, needing shorter length of the links with lower data rates for better optimization of the system in such environments [98].

In [99], error performance of FSO communications is given under clear but turbulent atmospheric conditions. Under these conditions, temperature variation means fluctuation in the irradiance. This research work considers the SIM-BPSK system. To analyze the performance of the system under different levels of turbulence, the received irradianceis modeled

using the gamma-gamma distribution. Spatial diversity is used to mitigate fluctuation caused by turbulence in the research. The conclusion states that for a bit error rate of $10^{-6}$ a signal-to-noise ratio of 29 dB is required in the case of weak turbulence, increasing with turbulence. The spatial diversity of two photodetectors can aggressively reduce the SNR requirement, with diversities of up to 21 dB in moderate and 16 dB in strong turbulence; however, the better the turbulence, the poorer the result [99]. The rapid fluctuations in position and intensity are the effects of beam instability due to atmospheric turbulence. This brings about the phenomena of beam wander, fading, and the random intensity variations, also known as scintillations. The fluctuations may cause intermittent data loss, increased error rates, and degraded communication quality. Communication traffic can be intercepted or an attack can be mounted which can cause partial loss of integrity and availability of a system, due to either communication loss or disrupted data gathering.

The performance of FSO Communications systems is evaluated in the [100] both for atmospheric conditions and different beam divergence and modulation schemes in the transmission of information. Variables environmental to the area like weather and variables environmental to the area like the smog in industry areas have a large effect on the bit rate of FSOC. These effects are analyzed using a simulation platform, which shows the relevance of the choice of transmission distance, as well as modulation schemes, to keep a certain BER level at $10^{-6}$ to $10^{-9}$. The results obtained indicate that the range is greatly reduced by beam divergence and atmospheric conditions, particularly fog. It was also pointed out in the paper that, with the use of either CWDM or DWDM in coarse or dense configurations, the bitrates can be increased a lot higher with the single-channel handicap toward the terabit-per-second limit [100].

The atmospheric disturbances may be corrected using adaptive optics, error-correction techniques, and real-time monitoring. One facility is the adaptive optics; it can adjust the focus of the beam real-time for the turbulence and scattering to be offset. Weather monitors provide data regarding visibility conditions to the systems, which causes the system to shift to another communication mode. In addition, error-correction technique of forward error correction and automatic repeat request is applied to ensuring data validly in degraded conditions. [101] addresses the problem of atmospheric turbulence in free-space optical communication systems by utilizing deep learning techniques at the transmitter, receiver, and transceiver sides for constellation shaping, detection, and joint constellation shaping-detection. Different structures based on deep learning are applied to MIMO FSO systems, where several combining schemes have been studied for a variety of turbulence conditions, ranging from weak to strong. The study concluded that DL-based methods achieve optimal performance in conventional FSO systems but with low complexity. Particularly, the proposed DL-based detector has a higher speed than the ML detector, which has 2, 3, and 7.5 times faster speeds than that of the latter for 16-, 64-, and 256-modulation orders, respectively. This therefore proves the efficiency and effectiveness of DL in mitigating atmospheric turbulence in FSO systems [101].

While such solutions enhance the best possible resistance in FSO systems, they are not completely infallible. In variable or unpredictable environments, even highly sophisticated mitigation strategies can have their limitations. This kind of assurance in any variable or unpredictable environment would require a multi-layered approach among performance, resilience, and security against a broad spectrum of environmental threats.

## IV. EXISTING SECURITY MECHANISMS

This section explains the current security mechanisms applied in FSO communication systems. This part of the paper deals in the encryption techniques, physical layer security, and authentication as well as key management. All these methods address problems and issues as well as the identified threats in order to have a smooth and risk-free communication in FSO links.

### *A. Encryption Techniques*

Encryption forms the backbone behind all the secure communications. This is realized in providing the aspect of confidentiality, since plain text is converted into the ciphered text with the help of the cryptographic algorithms. The major benefit that is attached to the parameter of encryption is that the data intercepted by unauthorized people would be rendered useless. The particular challenges, however, that are associated with the implementation of encryption in FSO include the following. Unlike other regular communication systems, FSO systems are typically utilized in the applications that possess low latency and minimum computational overhead properties. For example, the application in satellite communication or UAV relay networks is relevant to the requirement of real-time communication, which also requires much processing power, and an intense level of encryption algorithm should not make the procedure lag behind. Hence, any secure algorithm in use has to reflect good speed and high efficiency of resources. High processing and bandwidth ability is demanded by the fact that most of the FSO systems, thus, it is needed to use only those optimized encryption

algorithms with enough level of security taken place while the performance level is not dropped drastically .

FSO communications commonly use the Advanced Encryption Standard (AES) due to its secure algorithm, flexibility in key lengths (128, 192, or 256 bits), low computational overhead, and high speed, which is for applications that require high throughput. However, as AES is a symmetric key algorithm, i.e. the same key is shared between sender and receiver, key management in large or dynamic FSO networks can be challenging. To improve upon this, public-key algorithms like RSA are used for secure key exchanges. While RSA is good for secure key exchange in insecure channels, It needs high computation and is slower compared to AES and therefore less suitable for real-time encryption. Many FSO systems adopt a hybrid approach: RSA for key exchange and AES for data encryption. In scenarios demanding ultra-high security, such as military communications or financial transactions, additional encryption layers like elliptic curve encryption are sometimes combined with AES and RSA. However, these extra layers increase computational complexity, requiring careful trade-offs between security and performance. Realization in FSO systems needs to address trade-offs with the processing power between security and latency. Here, for most of the already available algorithms in AES or RSA, an increase in the length of elongation enhances the security in terms of complexity in brute force. However, this also gives a rise to computational overhead, making the encryption and decryption process slower. However, when coming to real-time performance needs, even this kind of a delay might be dramatically too much—for instance, in satellite communication or UAV networks.

Extensive study on encryption techniques have been conducted, and new algorithms devised. Following are a few studies catering to security in FSO Communication. Hughes1999 describes the development and testing of a free-space quantum key distribution system that will be used for secret key distribution using single-photon transmissions.It ensures secure exchange of cryptographic keys by utilizing non-orthogonal photon polarization states. Eavesdropping is made harder still through increased error rates during key exchange facilitating Secure key exchange. Tested on a 1 km optical link in the Los Alamos National Laboratory, the system proved that QKD can quite effectively provide secure real-time key distribution for confidential communications and has potential applications in surface-to-satellite QKD in the future [102]. [103] proposes a new two-dimensional encryption system of free-space optical (FSO) communicationthat utilizes spatial intensity and phase patterns as keys for encryption. The system is intended to encode binary data streams directly at the physical layer in order to provide an extra level of security: a successful encryption and decryption simulation is hereby confirmed. This is the first system in FSO where spatial patterns appear in the role of encryption keys, not data modulation [103]. [104] proposes a new method for quantum encryption in the coherent optical domain, designated as quantum encryption in the phase space (QEPS), employing the displacement operator for coherent states. It promotes security in transmission at rates of 56 Gbps for QPSK and 112 Gbps for 16-QAM over 80 km. They also demonstrate that the proposed encryption scheme is semantically secure in the wiretap channel model and can easily be implemented in a symmetric or asymmetric setup [104]. [105] highlights advancements in mobile Free-Space Optical (FSO) communication by the German Aerospace Center's Optical Communication Group. FSO links, offering high power efficiency and data rates, have been used for point to point links across platforms like aircraft, UAVs, and satellites. The research explores integrating standard FSO with quantum communication into a single optical terminal for secure, high-rate transmissions, aiming to demonstrate this via a LEO satellite downlink, potentially from the ISS [105]. [106] proposes a bit-level video frame cryptosystem via piecewise linear chaotic maps (PWLCMs) for orbital angular momentum modulation(OAM) through gamma-gamma turbulence channels. The accuracy of the proposed model is shown by comparing theoretical and simulation results and proving the system's security and robustness in different kinds of attacks. Further work will involve trying to integrate deep learning techniques with OAM for enhanced classification and prediction efficiency, and efficiencies of encryption and decryption [106]. [107] investigates the performance of an optical encryption scheme using the Random Phase Key transforms like Jigsaw Transform combined with QPS like Fourier, Fresnel, and Canonical transforms. In this paper, the Wigner distribution function assessment of spatial and frequency changes during encryption is done that affects the SBP. It proposes an automatic phase-space matrix method for guiding the selection of optical components with respect to SBP values and constraints of a system for optimum encryption and signal recovery [107].

For image transmission over the FSO, Choquet Fuzzy Integral (CFI) algorithm is utilized in below mentioned papers. [108] deals with a proposed scheme for secure image transmission over FSO channels using the Choquet fuzzy integral algorithm and integer wavelet transform, which is tested in different rain intensities over Alexandria, Egypt, and Jeddah, Saudi Arabia. The ranges of FSO decrease with increasing rainfalls. While for Jeddah, with its lower rainfall, it allows a maximum range of 8200 m. It further relays the security justification of the CFI algorithm through entropy and correlation analysis, making it feasible for secure image transmission in FSO links [108]. In [109], a secure image encryption method

is proposed using Choquet Fuzzy Integral for free space optics channels in the foggy environment. It isresistant to several types of attacks and thus has validation through metrics such as correlation coefficients, entropy, and key sensitivity. In this study, results comparing fog-affected plain and encrypted image transmission show that encryption can improve metrics like SNR and SSIM. This system has prime applications in the military and remote areas where laying optical fiber is not feasible for high-speed and secure communication [109]. Despite having specialized cryptosystems, the FSO Communication link might still be vulnerable to different attacks. [110] reports a successful interception of the RF radiation from the APDs in the QKD system, in which an eavesdropper could clone the quantum transmission data with more than 99% accuracy at a distance of up to 2 m. From these findings, one realizes that quantum cryptosystems are vulnerable to RF penetration attacks and therefore call for protection with more effective electromagnetic shields, closer coincidence of APDs, and installation of wideband jammers in quantum communication systems [110].

One of the other most important factors is the fact that there is security in the FSO communication itself. It is quite clear that the directionality of FSO links reduces the signal vulnerability to interception and opens up some possibilities for lighting certain encryption protocols to be used in some cases. On the other hand, the damage from a data breach in high-importance applications is generally quite high, and performance trade-offs cannot be tolerated; heavy encryption needs to be applied. Again, it needs precise knowledge about the application security needs, performance constraints, and environmental conditions for the selection of the encryption approach that would be appropriate.

### *B. Physical Layer Security Techniques*

The physical layer of FSO communication inherently offers security benefits due to the highly directional nature of optical beams. Unlike RF communications that scatter the signals everywhere in omnidirectional fashions, FSO beams actually narrow, and this fact becomes very difficult to intercept for an eavesdropper unless they are directly within the path of the beam, but it's still possible as discussed in [55]. Security will thus be assured to be better through the possibilities beam steering affords; that is, the determination of the direction of the beam to make it conform to the legitimate receiver's will while at the same time limiting its exposure to possible eavesdroppers. In cases of misalignments that could be due to atmospheric disturbances or mechanical vibrations because the platforms are usually not stationary, the importance of adaptive beam tracking systems cannot be overemphasized. Such systems realign the direction and focus of the beam in real time to keep the signal confined as much as possible in a secure path, minimizing the ease of intercepting it. These advanced methods in adaptive optics can continuously correct for the atmospherically induced disturbances, which is critical for the maintenance of the secure communication links.

Spatial diversity is the very strong possibility that can be used to enhance the reliability and security of the overall channel. By employing multiple beams, transmitters, or receivers, the information spreads over independentoptical ways which deny eavesdroppers access to the signal. This will be more applicable in mesh networks, where communication flows unimpededly through redundant paths in the case of one link being compromised. Another addition to this is the fact that techniques like time-domain scrambling make the intervals at which data packets are sent vary across the different beams.The same is achieved in security by the use of power control and adaptive modulation techniques. In power control, the power of transmission is varied with current environmental effects to close the optical beam, hence decreasing interception risks. In adaptive modulation schemes that adapt to changes in the real-time channel assessment, communication is secured by the actual introduction of variability that an eavesdropper has to estimate and decode. Though these techniques offer several security advantages, they also increase the complexity of both system design and management. For instance, processes like handling multiple beams and data synchronization are very complex and require sophisticated control algorithms, in addition to real-time processing, which is very resource-intensive. In many of these challenges, however, physical layer security is actually complemented quite often by encryption and authentication mechanisms at higher layers, and a multilayered defensive strategy may offer compensation to the weakness of any layer accordingly.

In [111], the intensity modulation/direct detection-based free-space optical communication physical layer security in the Málaga channels is studied. Three eavesdropper placement scenarios are considered, and novel expressions for average secrecy capacity and secrecy outage probability are derived in this paper. Some of the key observations from the results are as follows: (1) At the close vicinity of the transmitter, the detrimental effect of the atmospheric turbulence is less for secrecy (2) the effect of correlation can show the improvement and worsening of secrecy performance, it is non-monotonic (3) correlation influences the ASC and SOP differently with its influence being more prominent when the correlation is very low or high; and (4) the asymptotic slope of the SOP is 0.5 for all scenarios. The information helps make valuable contributions toward development and improvement in FSO communication security [111]. [112] discusses

the physical-layer security of FSO communication using OAM multiplexing in the presence of atmospheric turbulence. It is shown that OAM multiplexing can actually improve the aggregate secrecy capacity under weak- and medium-turbulent conditions in comparison with single-mode transmission. Additionally, it states that the performance is driven by the position of the eavesdropper, with greater risks when that eavesdropper gets closer to the transmitter. It also deduces that OAM multiplexing with expansion in a telescope requires more stringent conditions on the equipment of the eavesdropper. This paper concludes with a recommendation for more research regarding adaptive optics for further signal quality and secrecy capacity amelioration within OAM-multiplexed channels.

[113] presents experimental data in a free-space optical communication link on physical-layer security, obtained through a testbed simulating a typical scenario with a legitimate receiver and an eavesdropper. The concerned parameters, that is, those related to information theoretic metrics such as secrecy rate, the probability of secrecy outage, and expected code lengths, are experimentally evaluated under varying atmospheric conditions. The results appear as the variability of the secrecy rate in relation to the time of the day, having a more stable value during the hours of the evening and more variable during the sunset hours. This promises secure communication between distant nodes using PHY security combined with cryptographic techniques on layers located higher in the protocol stack, even if the conditions are strongly adverse. The findings have thus afforded a clear avenue toward field implementation of secure communication strategies, like secret key agreements, in real FSO systems, which will eventually lead to the large-scale deployment of PHY security in high-altitude and satellite-based communications. [114] investigates the prospects of Bessel-Gaussian beams in improving physical-layer security in free-space optics compared with that of Laguerre-Gaussian beams. The study further presented that BS beams, through computer simulations and experiments with spatial light modulators, do show higher secrecy capacities than other vortex beams do under weak to medium-strong turbulence conditions because of their enhanced resilience against atmospheric effects. This could permit more secure communication systems, provided that the Bessel-Gaussian beams can be optimized to that end [114].

For further knowledge you can refer [115], which presents a comprehensive survey on recent advances in PLS for RIS-enabled wireless systems in the context of future wireless technologies, specifically 5G and beyond. The review incorporates the analysis of RIS-enabled PLS scenarios and optimization techniques targeting the maximization of secrecy performance. More importantly, considering that the number of interactions is expected to increase with future networks, this will, consequently, be associated with increased complexity; it looks at the role that machine learning could play in managing the said complexity within RIS-assisted PLS-based systems. Finally, open research challenges and future research directions are identified and discussed of importance in extending the development and taking up RIS-assisted PLS into future wireless technologies [115].

### *C. Authentication Protocols and Key Exchange*

The authentication of identities of the communicating parties in Free-Space Optical (FSO) is a very significant step in ensuring that only legitimate users are in the picture of the key exchange. Without proper authentication, even secure key exchange protocols are open to impersonation attacks. The most common different kinds of authentication are multifactor protocols, public-key infrastructure (PKI), and digital certificates, which are usually paired with key-exchangeschemes in order to enhance security. Key exchange in FSO systems needs to be secure. This is due to the fact that symmetric key exchange schemes are normally combined with encryption protocols, such as AES, which are efficient through their high speed and low computational requirements. Nonetheless, large scale or dynamic network distribution without pre-shared key distribution is still quite challenging, particularly in military deployment or disaster responsive scenarios. Such protocols as RSA and Diffie-Hellman achieve key exchange through insecure channels, but the key agreement in these protocols is augmented with higher latencies and computational requirements. Hybrid systems often use asymmetric techniques for secure transport of the symmetric keys by binding the benefits of both methodologies. Hierarchical key management is necessary for such large-scale networks where the nodes move frequently—such as UAV swarms. This structure employs diverse key levels concerning various contexts of communication for flexible security. It is proper to verify the identities of entities while communicating with FSO. This is generally done using PKI, digital certificates, and cryptographic signatures. Mutual authentication enhances security, but with a higher delay. Lightweight authentication schemes that help reduce the number of handshakes steps and cryptographic operations without any compromise in security thus have been designed, especially for time-critical applications such as autonomous vehicles.

Key management must be robust in any dynamic FSO network where topology changes quite often. Handover and rekeying have to be secure to maintain the integrity of communication as nodes move in and out of the network. Auto-rekeying triggered by node movements or context changes is becoming increasingly prevalent but has to be designed

with minimum latency. Traditional centralized key management might work for small to medium scales, but it struggles to be scalable in large-scale networks, leading to interest in decentralized methods like blockchain for secure, scalable key distribution. Although theoretically sound, these advanced systems in key management and authentication will put in practical difficulties of cost, complexity, and specific hardware requirements, which practical FSO applications would need to optimize in future research and yet allow for the maintaining of security and scalability in communication under conditions that are complex and dynamic. There have been many studies conducted on Authentication and Key Exchange in the FSO Communication system. [116] paper considers an in-depth literature review on physical layer authentication for wireless communication networks; it analyzes 31 studies in the period 2015 to 2022. Of these, 45% of the studies are based on machine learning, whereas 55% are based on deep learning, and 69% of them are simulation-based. Furthermore, RF and channel characteristics almost share equal distribution for the implementation of PLA. The review discloses that while progress has been made, more studies are needed, particularly in the line of strengthening ML and DL techniques for wireless security [116]. [117] presents an authentication scheme in free-space communication using singular laser beams of a known order of singularity that generates a unique fingerprint pattern. At the receiver, a portion of the received beam interferes with a locally generated plane wave and is Fourier transformed to produce a frequency distribution pattern. This pattern is then captured by a CCD camera and compared with pre-stored patterns using application software. On successful matching, the 'high' signal is triggered and the digitized message passes through an AND gate. This approach not only provides secure authentication but also stability against stray light so that transmitted data in free space communication systems remains intact [117]. [118] integrates the concept of broadband access using Mobile WiMAX and Free Space Optics, considering FSO as a high-capacity backhaul where fiber deployment becomes difficult. In this paper, a single security framework using EAP is proposed, evaluating the protocols EAP-TLS and EAP-TTLS against each other. EAP-TTLS has been proven to be more efficient and secure, and there was no performance degradation in authentication due to the FSO link. The study proposes further testing on mesh networks of FSO in this integrated system [118].

In [119] , a Fabry-Perot cavity filter is proposed to separate orbital angular momentum beams from regular light in free-space optical communication. The filter selects the desirable modes, such as LG10, by properly setting cavity parameters even in very adverse atmospheric conditions. Simulations show high finesse and free spectral range for exact mode separation, hence providing communication stability. The approach can be used to filter other modes with additional design optimizations [119]. Two studies are done by Abdrabou and Gulliver on PLA for LEO satellites. [120] presents an adaptive physical layer authentication scheme for LEO satellites using machine learning, with Doppler frequency shift and received power features, to realize authentication accuracy of over 99.6%. This approach outperforms the existing methods, enhancing satellite security in vertical heterogeneous networks [120]. [121] deals with the physical layer authentication of LEO satellites by Doppler shift and received power for satellite-terrestrial network security. The hypothesis testing in this PLA scheme utilizes threshold methods or machine learning with one-class SVM training based on data from a legitimate satellite. Results show that while DS performs very well in low elevation angle cases, RP does so in high-angle situations. Machine learning can also improve authentication rates, especially due to the increase in training data and few outliers [121]. In [122], a quantum identity authentication scheme using the three-photon quantum error-avoiding code for noisy channels is presented. The system embeds information within a noiseless subsystem, which theoretically makes it robust to quantum noise and so very secure from the aspect of eavesdropping. This work has filled the lacuna of studies in antinoise quantum authentication and charted a road map toward improvements in the future [122]. Quantum Key Distribution is an emerging technology that will be discussed in detail in next section.

[123] proposes a private-key-based cryptosystem and key agreement scheme against physical layer security issues in air-to-ground free-space optical communication using turbulence-induced fading statistics. The derivation of the secret key rate via a gamma-gamma model illustrates that SNR and training sequence length have a significant impact on key generation. It will enhance the security features of FSO against eavesdropping by leveraging bidirectional channel measurements [123]. [124] proposes an optical information authentication system that integrates compressed, double-random-phase-encoded images with QR codes to provide improved security and sparsity of data. The parameters of the optical lightwaves would represent decryption keys, while the QR codes represent verification. Through iterative phase retrieval, one can easily perform DRPE encoding and decryption. It improves the security aspect and data efficiency of traditional Fresnel domain and conventional DRPE methods [124]. [125] addresses secret key distillation in the scenario of satellite-to-satellite free-space optics with an eavesdropper, Eve, who optimizes her position for power collection. Two cases are considered: Eve behind Bob, and Eve before Bob. For the long distances, Eve's optimal strategy is to align on the beam axis at Alice-to-Bob's distance; for shorter ranges, key rates as a function of distance depend on a

Bessel function integral. A suggested countermeasure is an exclusion zone. The results apply to Gaussian-modulated CV-QKD and DS-BB84 protocols, confirming Eve's optimal strategies and key rate bounds [125]. In [126], it demonstrated secret key agreement over a terrestrial free-space optics link of 7.8 km and analyzed the risk of eavesdropping. By virtually placing the eavesdropper near the receiver, this experiment represents the worst possible scenario, while only the signals that pass very strict criteria are used. Successful cases reached a key rate of 4 Mbps, which is the first demonstration of SKA over FSO channels, showing the need for robust methods against fading variability[126].

Diving to another emerging technology of blockchain [127] proposes a lightweight, multifactor mutual authentication protocol using ECC-based Diffie-Hellman and blockchain to improve security challenges in Cell-Free mMIMO for 6G. The proposed protocol improves security while drastically reducing the authentication and computational overheads by more than 50%. In the future, the authors would also like to integrate deep learning for efficient intrusion detection in a multihop environment.

## V. EMERGING SOLUTIONS

### *A. Quantum Key Distribution (QKD)*

Quantum Key Distribution has emulated how advanced technologies enhance threat detection. Arguably, quantum key distribution (QKD) is one of the most avant-garde advances in cryptographic security, leveraging quantum mechanics in its most primordial stage. Where the conventional use of mathematics and algorithms in cryptography might once again be cracked with enough computational power, QKD encodes cryptographic keys by use of quantum states, most notably photons. So here is the biggest advantage of QKD: the process is intrinsically secure. There will be a detectable disturbance of quantum states by eavesdropping, proving something happens. This, in turn, implies right from the beginning of QKD that it can be detected at the point of eavesdropping, and possibly the keys can be changed or aborted. In [128], the possibility of QKD over intersatellite links by considering a separate satellite hosting the entangled photon source enhances security and flexibility in quantum communication networks. The study concludes that such a setup for LEO satellites is attainable, as the link attenuation will be an important factor in keeping the security and preventing eavesdropping.[128]. [129] presents an overview of the integration of Free-Space Optics with Quantum Key Distribution for enhanced security in next-generation communications. Innovate-UK AIRQKD has explored metropolitan-scale, quantum-secure connectivity over FSO QKD links for high-performance, secure data exchange even in rural areas. The project shall prove that FSO-QKD complements the existing technologies for end-to-end secure provision without use of fiber, overcoming the threats such as line-of-sight requirements and ensuring strong performance in a real environment [129].

High directionality within FSO systems and large capacity for conveying quantum states with minimal interferences underline the suitability of FSO for QKD. The result of this is the possibility of optical beams to be tightly transmitted in FSO links, guaranteeing a very low probability of interception. Besides that, the current line-of-sight implementation is rather well matched with requirements needed for quantum signal propagation. This makes use-cases of FSO in QKD extremely interesting and relevant to government, military, and finance applications, where long-distance secure communication is of crucial importance. [130] presents, for the first time, a real-time entangled photon-based QKDsystem over two free-space links covering a distance of 1,575 meters. Using the BBM92 protocol, a secure key rate of 85 bits/s was achieved with an average quantum bit error rate of 4.92% for more than six hours of night operation [130].

[131] describes a free-space QKD system using attenuated laser pulses over 480 meters, suited for continuous unattended operation. The system in its current state operates during nighttime and produces sifted keys at rates well above 50 kbit/s with quantum bit errors of 3-5%. Future improvements will be in the temperature stabilization, addition of spectral filters for operation in daylight, and incorporation of authentication and decoy states protocols for enhanced security and higher key rates [131]. [132] reports on the first experimental realization of a BB84 quantum key distribution protocol over a 144 km free-space link using weak coherent laser pulses. Our implementation established a secure key rate of 11 bits/s for attenuation of 35 dB, simulating conditions for satellite downlinks. This demonstrates the feasibility of satellite-based QKD, thus paving the way for the realization of a global quantum communication network [132]. In [133], the authors present QKD with time-bin encoded photons under turbulence-induced distortions and depolarization within a free-space channel of length 1.2 km. This system achieves a stable quantum bit error ratio of about 5.32%, yielding secure-key generation at rates of up to 154.2 bits/s using a novel analyzer. This experiment proves the feasibility of time-bin quantum communication in turbulent free-space and thus makes available the potential for its seamless integration into both fiber and free space quantum networks to support advanced protocols over long distances [133].

Many QKD schemes have been devised, with the BB84 being the most widely researched and effectively employed. The BB84 scheme involves a sender, Alice, and a receiver, Bob, who send messages to each other; in this transmission, both Alice and Bob send and receive polarized photons to represent bits of an encryption key. From the strange quantum properties of photons that have been discussed, Alice and Bob realize that if they perform key exchange, there is eavesdropping taking place. The key is now secure, and later, what comes after can be utilized for different communications between the two parties. In the realization of an FSO system, polarization photons pass through an optical channel that has the high-bandwidth and low-latency application of the FSO link. BB84 is also implemented. Current modern system technology in recent systems is based on satellite QKD, in which FSO systems are implemented with satellites to achieve QKD over long distances. An experimental implementation of a fully automated Quantum Key Distribution system based on the BB84 protocol is presented in [134]. The low quantum bit error rate of about ~1.2% demonstrated by a system using a weak coherent pulse source for the generation of polarization-encoded single photons corresponds to a generation rate of a sifted key at ~70 Kbps. Finally, this will yield after post-processing a secure key rate of around ~33 kbps. The system demonstrates unconditional security for image communication within an unsecured public channel. Further work on the said improvement targets the increase in key generation rates and optimization of software for performance enhancements [134]. [135] presents a free-space implementation of quantum key distribution using the BB84 protocol with attenuated laser pulses that features the highest sifted key rate to date, at 23.6 kbit/s, and very low quantum bit error rate of 3%, which is insusceptible to added channel losses. The system, built from commercially available components, is being further developed with decoy-state methods and FPGA-based electronics for continuous operation, and with the present upgrade plan testing at ordinary conditions will end up showing good practical potential and capability for long-distance QKD [135].

The protocols make use of quantum key distribution, including entanglement, such as the Ekert91. Many of these protocols exhibit better security features because they cannot be attacked with attack types, including photon number splitting attacks; therefore, they offer a significantly improved overall security degree for systems based on quantum key distribution. Such protocols are being widely used in quantum key distribution-based free-space optical communication due to an increased interest from researchers and developers with the aim of achieving performance enhancement, large area coverage, and scalability. In [136], the authors present the practical scheme for the implementation of the high-dimensional KMB09 quantum key distribution protocol. The latter allows long-distance communication due to encoding of the secret bits into higher-order Gaussian beam spatial modes. Simulation has been done for two- and four-dimensional photon states, and efficiencies of 0.25 and 0.3683, respectively, were obtained in correspondence with the analytical calculation [136].

While this may seem very promising, several pragmatic challenges exist in practice for quantum key distribution using free-space optics. First of all is that the two parties between whom communication is happening require close alignment. As already described earlier, the quantum states are highly disturbed by disturbances and every misalignment in the optical beam may establish either greatly lost signals or high error probabilities. The tolerances required in effective permission of the transmission for the narrow FSO beam are excessively large in transportation of quantum states. [137] proposes the Adaptive Real Time Selection (ARTS) technique to bypass the effects of the atmospheric turbulence in quantum key distribution (QKD) over free-space channels. By selecting those with the higher channel transmissivity in real time, the ARTS method allows secure key generation under conditions when the average QBER would be too high. The proposal is demonstrated to work effectively in the 143-km free-space link experiment [137]**.** In [138] , a multiphoton quantum key distribution protocol deploying a multi-beam free-space optics setup is proposed to reduce geometrical loss and achieve better performance under atmospheric turbulence. Present analysis indicates that such a scheme may reduce the channel loss by about 8 dB besides lowering the quantum bit error rate (QBER) and raising the secret key rate (SKR) compared to its single-beam counterpart, thereby making it more effective in long-distance quantum communication [138]. In [139] , Photon Key Distribution is put forward as an alternative of quantum key distribution in free-space quantum communications, especially for satellites. Assuming that the man-in-the-middle attack could be detected classically, protocols and hardware could be simplified by PKD. Doubled key rates are achieved by using only one measurement basis and allowing key generation even at higher losses. The work can therefore improve the secure key distribution in scenarios such as satellite links and ad-hoc networks where security risks are typically lower [139].

The quantum signals degrade with the introduction of several other functionalities with the atmospheric conditions such as turbulence, fog, rain, and scattering. It results in the weakening where the effectiveness of the signal becomes limited

either on the free-space optical link. However, a different challenge remains in the high cost and complexity that comes together with all QKD systems. This is explained by a relatively high cost of QKD implementation since the used special quantum hardware is used in a state of art: single-photon detectors and quantum random number generators. Stable support of quantum communication can result in high complexity of error corrections over large distances or under operating settings that assume a dynamically changing environment for signal processing. In order to extend the QKD range in FSO communication, the details of quantum error correction code and repeaters development are to be furnished. One needs to bound the effort in hybrid quantum–classical systems and exploit security enhancement through QKD while robust operation ensues from classical encryption. This is practical work based on real-world application interest and development technique for providing a practical scalable solution. To gain more information regarding QKD, [140] can be referred to. It provides a summary and reference to the development and implementation of QKD over FSO links for both terrestrial and satellite communication. While doing so, this paper does highlight recent improvements, compares different QKD protocols, and discusses future perspectives and challenges towards accomplishing a global secure quantum network, possibly with its integration towards PLC for UAV mobile networks as well [140].

***B. Machine Learning for Security***

The inclusion of Machine Learning (ML) within FSO communication systems is progressively providing an edge to the solution by detecting threats in real time and changing the defense strategy. Conventional security mechanisms deployed in FSO systems greatly rely on predefined policies and static algorithms and, thus, when exposed to evolving complex and dynamic cyber threats, such mechanisms turn out to be inefficient.On the contrary, big data can easily be processed by ML, harvesting inferences from emerging trends and programmatically making decisions through which anticipatory defense methods may be anticipated. Machine Learning (ML) has seen a significant impact on Optical Communication (OC), but few OC experts are familiar with suitable ML algorithms. In [141] , authors have given a comprehensive review from the ML perspective to give insights to the OC researchers with more studies as compared to previously surveyed works [141].

These varieties of ML models constantly scan in FSO systems, overrunning to detect jamming attacks, unsolicited interception, or signal attenuation because of environmental factors. Such models give a monitoring watch over the communication channel all the time against any kind of subtle change and are emulated as if some kind of security breach has occurred. For example, it can be ascertained whether there is any change in signal strength because of atmospheric changes or the same change is being induced because of some form of interference created deliberately.This beam responds to the identification of a potential threat by automatically realigning, adjusting in the power in the transmission, changing the communication mode, or making any other necessary adjustments. [142] compares various machine learning methodologies, including ANNs, support vector machines, and logistic regression, for the detection of power jamming attacks in optical networks. This investigation has shown that ANNs perform best in the detection of out-of-band jamming attacks. Further, this paper proposes a resource reallocation scheme to mitigate such kinds of attacks by reducing the probability of successful jamming attacks, enhancing data security in optical networks [142]. [143] justifies the use of classical channel models to describe statistical fluctuations in satellite-to-ground quantum atmospheric channels, particularly under weak turbulence and pointing errors. Specifically, the analysis of quantum bit-error rates (QBERs) and secret-key lengths (SKLs) are presented for a CubeSat-based QKD link, and the importance of stable beam pointing for maintaining good performance. Related to this is the provided deep-learning-based method, whose system will predict the photon count's fluctuation using LSTMs RNN and direct the element that has to be improved in order to have good performance in real-time predictions [143].

The work in [144] introduces a simplified photonic RC scheme for the classification of highly distorted optical communication signals; it significantly enhances the bit-error-rate and extends the range of communications. This scheme processes the signal that is impaired deterministically during the transmission and is routinely enhanced for advanced modulation formats, but the ability to process in real-time at the telecom rates is still a complex task [144]. The work of

[145] discusses the different techniques to mitigate turbulence-induced fading in free-space optical communication links. It discusses the use of maximum likelihood detection to improve signal detection when the receiver has knowledge of either the marginal or joint temporal statistics of the fading. Spatial diversity reception with multiple receivers as a means of alleviating the effects of fading is also investigated where ML detection results in better performance than conventionalapproaches, especially when fading across receivers is correlated [145].

Of course, the benefit behind this is that ML-based security can only get stronger as time goes on: the more new models on attack vectors are brought in by the modern dataset during training, the better ability the model will have to detect and

protect against new threats. This puts the system right at the cutting edge of thinking about changing security landscapes. Many machine learning methods are implemented with the purpose of improving the integrity of FSO systems. Typical supervised algorithms are decision trees and support vector machine-based models, which classify communication patterns to show the presence of different threats. Such models require supervised data, which should be manually labeled, with normal and anomalous behaviors to be further distinguished for both supporting the training process of the models and learned classification in practice. These are unsupervised learning algorithms of clustering and anomaly detection; hence, they target the identification of completely new threats. That is to say, the models don't really rely on labeled data but rather look for deviations from a normal behavioral pattern. In this way, the system will be in a position to help the FSO link to indicate a set of strange patterns, related to fluctuations of signals as a possible attack, when that exact pattern was never seen before.

[146] focuses on QKD for securing IoT deployments, especially against quantum-capable adversaries. This work introduces an algorithm and machine learning techniques, such as ANN and LSTM, toward the detection of attackers with 99% accuracy without interfering in the QKD process. A use case related to securing IoT communications in railroad networks is also discussed [146]. [147] shows that ML has great potential and performance in various stages of continuous-variable quantum key distribution, outperforming the conventional algorithms in noise filtering, parameter optimization, and system estimation. In spite of some traditional methods that work equally well, ML is positioned as a strong tool to promote real-time CV-QKD toward practical implementation [147]. [148] rephrases the problem of attack detection in smart grids as a machine learning problem. The performance of several supervised, semi-supervised, and online learning algorithms used to detect attacks in smart grids is analyzed under various attack scenarios. The results show that machine learning tools, specifically support vector machines and k-nearest neighbors, perform better than traditional state vector estimation approaches both for observable and unobservable attacks. Such research underlines the impact of system size, data sparsity, and kernel selection on algorithm performance; though fusion methods attain greater robust performance, they are of higher computational complexity. Semi-supervised methods are resilient to the effects of data sparsity [148].

More experimental reinforcement learning can further be applied to reinforcing security in FSO. This system learns experiences interacting with the ever-changing environment. It can, therefore, be adaptive enough for general consideration in dynamically complex conditions like reconfiguring alignment or power levels and raising efforts against jamming. The system based on ML remains better with time while making its strategies safe from all sorts of threats, known and underbred. Additionally, in the case of FSO applications, there are extreme variabilities in the availability of labeled datasets if and when ML models are deployed. These add considerably to the dynamics of the FSO links brought about by changing climatic variations and movements and obstructions in the environment. Thus, researchers have been trying to find a way out through synthetic data generation, transfer learning, and domain adaptation towards achieving high accuracies with the robust ML models in the FSO security domain. [149] investigates a machine learning (ML) framework for detecting and identifying physical-layer attacks in optical networks using an experimental dataset from a testbed with coherent receivers. Among the eight classifiers tested, ANN yielded an accuracy of 99.9 percent success and handled large volumes of data sets simultaneously. The authors conclude by stating that a critical task is to identify the key Optical Performance Monitoring parameters that can enable the correct and efficient detection of an attack. The overall conclusion drawn is that the proposed framework has a significant potential to make optical networks more secure, with challenges for real-world implementation and integration to existing systems being future plans [149].

In the future there might be AIML based FSO security models that are much more fleshed-out to operate with very low human presence. Another interesting line of study concerns federated learning, which is where AI models are so trained over a gargantuan set of nodes that they are, in effect, decentralized by techniques that make training private and allow the detection of threats when combined over a distributed network. Modern optical communication networks represent a developing complexity that requests techniques for smarter and adaptive management. Consequently, machine learning goes hand in glove with various research works. [150] reviews ML techniques applied to optical networks pointing out existing research and proposing new directions to further advance the field [150]. The combination of AI-driven security and quantum-based solutions, paves the way for predictive defense in depth against cyber attacks that maybe could cause mass damage. It essentially means that as the AI models evolve into something advanced, there needs to be a juncture where they reduce computational complexity to at least meet the requirements for real-time systems in FSO. Simple, lightweight algorithms optimized for the respective environments with resources are a perfect way of ensuring seamless infusion into FSO systems without hiccups in performance or any latency overhead.

### *C. Hybrid Systems for FSO Communication*

Hybrid networks are attempts to allow the sum of the strengths of the various sets of communication technologies to perform in a manner that offers greater coverage, reliability, and general performance. Then comes the problem of FSO technology, combined with several other communication technologies, for instance, RF and fiber optics. A new single security challenge is how to keep the uniform security all across. After all, seamless link in the security handover from FSO to RF to the fiber technology is indeed critical. [151] proposes and studies the novel design of a hybrid FSO/RF antenna based on a modified Cassegrain antenna, where the aim is to accommodate both RF and FSO transceivers for high-speed access networks. In this design, the transmit and receive optical apertures have been separated to help improve propagation under turbulence channels. The proposed antenna design demonstrated good efficiency, easier alignment, better link performance for longer distances, and was effectively operational for a 1 km link verified through simulations and experiments [151]. [152] proposes a novel coding mechanism using nonuniform and rate-compatible LDPC codes that are able to enhance the reliability in hybrid FSO/RF communication systems without data duplication on the RF channel. The proposed scheme significantly improved bit error rates and reduced outage probabilities while preserving the security advantages of FSO communications. The work shows the possibility of achieving carrier-grade reliability (99.999%) in FSO links and points to further studies of integrating rate compatibility for a fully hybrid communication system [152].

FSO Communication has a lot of advantages like high data capacity and bandwidth, which makes it feasible for several applications like cellular backhaul and satellite communication. At the same time, the performance of FSO is highly affected by the atmospheric turbulence as well as weather conditions. A lot of recent studies are aimed at investigating hybrid modulation schemes towards better performance of FSO and decreasing the bit error rate or increasing bandwidth efficiency. [153] reviews FSO channel models, mitigation techniques, and the progress of hybrid modulation schemes, therefore pointing to further research across different communication layers [153]. A survey, [154] infers that hybrid FSO/RF systems usually perform much better than stand-alone FSO or RF systems, for worse weather conditions. This is because it uses many links to achieve higher reliability and performance. The advantages of hybrid systems to satisfy the demand for high speed, high capacity from the modern communication network, due to incompetence in atmospheric conditions, put them into light. It should be noted that, with continuous progress, FSO will definitely be involved in the future in telecommunications [154].

It is interesting that a transition break would expose the network to attackers like man-in-the-middle or unauthorized access. Additionally, differences at the physical and protocol level are likely to make the security policy determination inconsistent between FSO and RF/fiber, thus leaving an easy loophole for the attacks to succeed. For example, a FSO's natural feature is being interference-proof, while an RF system, being natural, is easily prone to jamming/eavesdropping. Now, the introduction of security mechanisms between the environments would provide the much-needed care in making the protocols of encryption, authentication, and key management harmonized to be equally robust along with intrusion detection. New integrated key management systems are now being developed that will support both FSO and RF/fiber channels. The security mechanisms operating at cross layers must keep those authentication credentials as well as the encryption keys constant across any communication path. This therefore enhances the coordination to strengthen risk mitigation as much as possible throughout the handover procedure. An instance in which synchronization across channels is done in a way that maintains encryption keys and security states, hence avoiding any leakage, is the secure handover protocol. Powerful solutions based on the same are the security policies that are adapted dynamically according to the network state. [155] proposes a secure hybrid RF/FSO transmission scheme that takes advantage of the merits of both RF and FSO links to improve the secrecy performance. It designs two kinds of policies: an FSO dominant secure policy, which schedules the FSO link with priority because of its higher secrecy performance, and an Secrecy Rate Optimal policy that selects between FSO and RF links optimally based on their secrecy rates. Numerical results confirm improved secrecy performance of both policies [155]. In [156], secrecy performance of hybrid satellite and Free-Space Optical (FSO) cooperative communication systems is considered with the different fading distributions and detection techniques. The derivation of the analytical expressions of average secrecy capacity (ASC) and secrecy outage probability (SOP) for both amplify-and-forward (AF) and decode-and-forward (DF) relaying schemes are derived. Results indicate that the satellite link greatly influences the secrecy performance, where for AF systems, FSO link, and detection methods affect the secrecy diversity order while for DF systems, it becomes zero [156].

This kind of protection scheme needs a constant recon-figuration at all instants in time. Their monitoring stays tothe same level of protection, whereby only communication paths shift between FSO link, RF link, and fiber path. For instance, in poor weather, where the FSO performance degrades terribly, the system can shift over to the RF spare and, of course, stay at the same level of protection.

## VI. CONCLUSION

FSO communication is promising in offering high data rates, low latency and decreased power consumption. However, it has problems associated with the open-air nature of FSO links, susceptibility to eavesdropping, jamming, and physical layer attacks. The security protocols discussed ranged from methodologies of encryption to defenses at the physical layer and even other recent breakthroughs, such as Quantum Key Distribution (QKD), and the application of Artificial Intelligence and Machine Learning techniques in the advancement of FSO security.

Although several significant security breakthroughs have been made in the recent past on FSO communication, key research gaps mainly persist as the standardized security protocols tailored toward specific FSO needs. These gaps can only be filled with further research. Future work should focus on reinforcing security frameworks and giving momentum to the use of AI and machine learning for the detection of threats and the critical integration of robust encryption mechanisms in order to enable FSO technology to ensure that FSO technology can meet the growing demands of secure, high-speed wireless communication in various fields. There is a real need to focus the research gaps based on such challenges to provide strong solutions for coping with the identified challenges in FSO communications, with the ultimate aim of real secure deployment of FSO systems into different applications.

## REFERENCES

[1] Raj, A. Arockia Bazil, et al. "A review–unguided optical communications: Developments, technology evolution, and challenges." Electronics 12.8 (2023): 1922.

[2] Ghassemlooy, Zabih, Arun Majumdar, and Arockia Bazil Raj. "Introduction to free space optical (FSO) communications." (2019): 1-26.

[3] Pradhan, Jagdish, et al. "Free Space Optical Communication (FSO)." International Journal of Engineering & Technology 4.4 (2017).

[4] Sadiku, Matthew NO, Sarhan M. Musa, and Sudarshan R. Nelatury. "Free space optical communications: an overview." European scientific journal 12.9 (2016): 55-68.

[5] Zafar, Saima, and Hira Khalid. "Free space optical networks: applications, challenges and research directions." Wireless Personal Communications 121.1 (2021): 429-457.

[6] Malik, Aditi, and Preeti Singh. "Free space optics: current applications and future challenges." International journal of optics2015.1 (2015): 945483.

[7] Jahid, Abu, Mohammed H. Alsharif, and Trevor J. Hall. "A contemporary survey on free space optical communication: Potentials, technical challenges, recent advances and research direction." Journal of network and computer applications 200 (2022): 103311.

[8] Chaudhry, Aizaz U., and Halim Yanikomeroglu. "Free space optics for next-generation satellite networks." IEEE Consumer Electronics Magazine 10.6 (2020): 21-31.

[9] Kedar, Debbie, and Shlomi Arnon. "Urban optical wireless communication networks: the main challenges and possible solutions." IEEE Communications Magazine 42.5 (2004): S2-S7.

[10] Zhang, Guoqiang, et al. "A Review of Variable-Beam Divergence Angle FSO Communication Systems." Photonics. Vol. 10. No. 7. MDPI, 2023.

[11] Arockia Bazil Raj, A., et al. "Mitigation of beam fluctuation due to atmospheric turbulence and prediction of control quality using intelligent decision-making tools." Applied optics 53.17 (2014): 3796-3806.

[12] ArockiaBazilRaj, A., & Darusalam, U. (2016). Performance improvement of terrestrial free-space optical communications by mitigating the focal-spot wandering. Journal of Modern Optics, 63(21), 2339–2347. https://doi.org/10.1080/09500340.2016.1200684

[13] ArockiaBazilRaj, A., and Ucuk Darusalam. "Performance improvement of terrestrial free-space optical communications by mitigating the focal-spot wandering." Journal of Modern optics 63.21 (2016): 2339-2347.

[14] Obeed, Mohanad, et al. "Survey on physical layer security in optical wireless communication systems." 2018 seventh internationalconference on communications and networking (ComNet). IEEE, 2018.

[15] Krelina, Michal. "Quantum Communication Countermeasures." arXiv preprint arXiv:2310.08728 (2023).

[16] Raj, Arockia Bazil, and Arun K. Majumder. "Historical perspective of free space optical communications: from the early dates to today's developments." Iet Communications 13.16 (2019): 2405-2419.

[17] Patle, Nidhi, et al. "Review of fibreless optical communication technology: History, evolution, and emerging trends." Journal of Optical Communications 45.3 (2024): 679-702.

[18] Raj, A. Arockia Bazil. Free space optical communication: system design, modeling, characterization and dealing with turbulence. Walter de Gruyter GmbH & Co KG, 2015.

[19] Joseph, Chinchu, and Appala Venkata Ramana Murthy. "Design and Implementation of a Visible Light Communication System for Indoor Environment." ICOL-2019: Proceedings of the International Conference on Optics andElectro-Optics, Dehradun, India. Springer Singapore, 2021.

[20] Saadi, Muhammad, et al. "Design and implementation of secure and reliable communication using optical wireless communication." Frequenz 68.11-12 (2014): 501-509.

[21] Ho, Tzung-Hsien, et al. "Studies of pointing, acquisition, and tracking of agile optical wireless transceivers for free-space optical communication networks." Optics in Atmospheric Propagation and Adaptive Systems VI. Vol. 5237. SPIE, 2004.

[22] Ho, Tzung-Hsien, Stuart D. Milner, and Christopher C. Davis. "Fully optical real-time pointing, acquisition, and tracking system for free space optical link." Free-Space Laser Communication Technologies XVII. Vol. 5712. SPIE, 2005.

[23] Plank, Thomas, et al. "Wavelength-selection for high data rate Free Space Optics (FSO) in next generation wireless communications." 2012 17th European Conference on Networks and Optical Communications. IEEE, 2012.

[24] Rockwell, David A., and G. Stephen Mecherle. "Wavelength selection for optical wireless communications systems." Optical Wireless Communications IV. Vol. 4530. SPIE, 2001.

[25] Anandkumar, D., and R. G. Sangeetha. "A survey on performance enhancement in free space optical communication system through channel models and modulation techniques." Optical and Quantum Electronics 53.1 (2021): 5.

[26] Bibi, Sannia, et al. "A comprehensive survey of free-space optical communication–modulation schemes, advantages, challenges and mitigations." Journal of Optical Communications 0 (2023).

[27] Du, Silun, et al. "Communication Performance of OAM Based FSO System in Weak Turbulence Environment." 2022 IEEE 10th International Conference on Information, Communication and Networks (ICICN). IEEE, 2022.

[28] Sharma, Nikhil, and Parul Garg. "Cross-QAM signaling in free space optical communication systems with generalized pointing errors." 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall). IEEE, 2017.

[29] Li, Zhixiang, et al. "High-efficiency anti-interference OAM-FSO communication system based on Phase compression andimproved CNN." Optics Communications 537 (2023): 129120.

[30] Du, Silun, et al. "Communication Performance of OAM Based FSO System in Weak Turbulence Environment." 2022 IEEE 10th International Conference on Information, Communication and Networks (ICICN). IEEE, 2022.

[31] Monteiro, Eric, and Steve Hranilovic. "Design and implementation of color-shift keying for visible light communications." Journal of Lightwave Technology 32.10 (2014): 2053-2060.

[32] Becerra, Raimundo, et al. "A Wavelength-Dependent Visible Light Communication Channel Model for Underground Environments and Its Performance Using a Color-Shift Keying Modulation Scheme." Electronics 12.3 (2023): 577.

[33] Guo, Meng, et al. "Design and analysis of color shift keying modulation based cooperative SM VLC system." 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2020.

[34] Kaushal, Hemani, and Georges Kaddoum. "Free space optical communication: challenges and mitigation techniques." arXiv preprint arXiv:1506.04836 (2015).

[35] Raj, A. Arockia Bazil, and S. Padmavathi. "Quality metrics and reliability analysis of laser communication system." Defence Science Journal 66.2 (2016): 175-185.

[36] Anthonisamy, Arockia Bazil Raj, and Arputha Vijaya Selvi James. "Formulation of atmospheric optical attenuation model in terms of weather data." Journal of Optics 45 (2016): 120-135.

[37] Bazil Raj, A. Arockia, and J. P. Lancelot. "Seasonal investigation on prediction accuracy of atmospheric turbulence strength with a new model at Punalkulam, Tamil Nadu." Journal of Optical Technology 83.1 (2016): 55-68.

[38] Raj Anthonisamy, Arockia Bazil, Padmavathi Durairaj, and Lancelot James Paul. "Performance analysis of free space optical communication in open-atmospheric turbulence conditions with beam wandering compensation control." IET Communications 10.9 (2016): 1096-1103.

[39] Eguri, Samson Vineeth Kumar, Arockia Bazil Raj A, and Nishant Sharma. "Survey on acquisition, tracking and pointing (ATP) systems and beam profile correction techniques in FSO communication systems." Journal of Optical Communications 0 (2022).

[40] Joseph, Chinchu, et al. "A Linear Closed Loop Feedback System for Beam Wander Correction in Medium-Range Optical Link." 2023 IEEE Pune Section International Conference (PuneCon). IEEE, 2023.

[41] Raj, A. Arockia Bazil, J. Arputha Vijaya Selvi, and D. Kumar. "Low cost BER measurement in wireless digital lasercommunication link with autonomous beam steering system." ICWCSC (2010): 1-6.

[42] Biswas, Abhijit, et al. "Status of NASA's deep space optical communication technology demonstration." 2017 IEEE International Conference on Space Optical Systems and Applications (ICSOS). IEEE, 2017.

[43] Hassan, M. Mubasher, and G. M. Rather. "Free space optics (FSO): a promising solution to first and last mile connectivity (FLMC) in the communication networks." IJ Wireless and Microwave Technologies 4.1 (2020): 1.

[44] Majumdar, Arun K., et al. "Optical networks, last mile access and applications." Free-space laser communications: principles and advances (2008): 273-302.

[45] Sabri, Atheer A., Samir M. Hameed, and Wael AH Hadi. "Last mile access-based FSO and VLC systems." Applied Optics 62.31 (2023): 8402-8410.

[46] Leitgeb, Erich, et al. "High reliable optical wireless links for the last mile access." 2008 10th Anniversary International Conference on Transparent Optical Networks. Vol. 4. IEEE, 2008.

[47] Tezergil, Berke, and Ertan Onur. "Wireless backhaul in 5G and beyond: Issues, challenges and opportunities." IEEE Communications Surveys & Tutorials 24.4 (2022): 2579-2632.

[48] Abdelmoaty, Ahmed, et al. "When Resiliency Matters: An Overview of 5G and Beyond Wireless Backhaul NetworkDesign." IEEE Communications Magazine 61.12 (2023): 206-212.

[49] Alzenad, Mohamed, et al. "FSO-based vertical backhaul/fronthaul framework for 5G+ wireless networks." IEEE Communications Magazine 56.1 (2018): 218-224.

[50] Jeyaseelan, Jeyarani, D. Sriram Kumar, and B. Elizabeth Caroline. "Disaster management using free space optical communication system." Photonic Network Communications 39.1 (2020): 1-14.

[51] Wu, Di, Xiang Sun, and Nirwan Ansari. "An FSO-based drone assisted mobile access network for emergency communications." IEEE Transactions on Network Science and Engineering 7.3 (2019): 1597-1606.

[52] Raghavan, Rajesh S., Ambrose Kam, and Rao Y. Mannepalli. "Modeling & simulation to study the performance of hybrid free space optical/rf military communication networks." MILCOM 2008-2008 IEEE Military Communications Conference. IEEE, 2008.

[53] Juarez, Juan C., et al. "Free-space optical communications for next-generation military networks." IEEE Communications Magazine 44.11 (2006): 46-51.

[54] Kumar, Suresh, and Nishant Sharma. "Emerging military applications of free space optical communication technology: A detailedreview." Journal of Physics: Conference Series. Vol. 2161. No. 1. IOP Publishing, 2022.

[55] Zou, Difan, and Zhengyuan Xu. "Information security risks outside the laser beam in terrestrial free-space optical communication." IEEE Photonics Journal 8.5 (2016): 1-9.

[56] Lopez-Martinez, F. Javier, Gerardo Gomez, and José María Garrido-Balsells. "Physical-layer security in free-space optical communications." IEEE Photonics Journal 7.2 (2015): 1-14.

[57] Bashir, Muhammad Salman, and Mark R. Bell. "Optical beam position estimation in free-space optical communication." IEEE Transactions on Aerospace and Electronic Systems 52.6 (2016): 2896-2905.

[58] Bashir, Muhammad Salman, and Mark R. Bell. "Optical beam position tracking in free-space optical communication systems." IEEE Transactions on Aerospace and Electronic Systems 54.2 (2017): 520-536.

[59] Sidorovich, Vladimir G. "Optical countermeasures and security of free-space optical communication links." Advanced Free-SpaceOptical Communications Techniques and Technologies. Vol. 5614. SPIE, 2004.

[60] Lahari, Sreerama Amrutha, ArockiaBazil Raj, and S. Soumya. "Control of fast steering mirror for accurate beam positioning in FSO communication system." 2021 International Conference on System, Computation, Automation and Networking (ICSCAN). IEEE, 2021.

[61] Qi, Yang, et al. "Free-space optical stealth communication based on wide-band spontaneous emission." Optics Continuum 1.11 (2022): 2298-2307.

[62] Savino, Nicholas J., Sanjaya Lohani, and Ryan T. Glasser. "Deep learning for eavesdropper detection in free-space optical ON-OFF keying." Optics Continuum 1.12 (2022): 2416-2425.

[63] Aveta, Federica, Hazem H. Refai, and Peter G. LoPresti. "Number of users detection in multi-point FSOC using unsupervised machine learning." IEEE Photonics Technology Letters 31.22 (2019): 1811-1814.

[64] Monteiro, Marcos Eduardo Pivaro, et al. "Effective secrecy throughput analysis of relay-assisted free-space optical communications." Physical communication 35 (2019): 100731.

[65] Trinh, Phuc V., et al. "Secrecy analysis of FSO systems considering misalignments and eavesdropper's location." IEEE Transactions on communications 68.12 (2020): 7810-7823.

[66] Erdogan, Eylem, et al. "The secrecy comparison of RF and FSO eavesdropping attacks in mixed RF-FSO relay networks." IEEE Photonics Journal 14.1 (2021): 1-8.

[67] Chaiwongkhot, Poompong, et al. "Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence." Physical Review A 99.6 (2019): 062315.

[68] Paul, Pratiti, and Manav R. Bhatnagar. "Jamming threats in free-space optics." IEEE Communications Magazine 60.12 (2022): 104-108.

[69] Paul, Pratiti, Manav R. Bhatnagar, and Anshul Jaiswal. "Jamming in free space optical systems: Mitigation and performance evaluation." IEEE transactions on communications 68.3 (2019): 1631-1647.

[70] Paul, Pratiti, and Manav R. Bhatnagar. "DF relaying in cooperative free space optical communication system in presence of jammer." 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP). IEEE, 2020.

[71] Agaskar, Manishika, and Vincent WS Chan. "Nulling strategies for preventing interference and interception of free space optical communication." 2013 IEEE International Conference on Communications (ICC). IEEE, 2013.

[72] Paul, Pratiti, Manav R. Bhatnagar, and Anshul Jaiswal. "Performance of free space optical communication system under jamming attack and its mitigation over non-gaussian noise channel." 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). IEEE, 2019.

[73] Paul, Pratiti, Manav R. Bhatnagar, and Anshul Jaiswal. "Alleviation of jamming in free space optical communication over Gamma-Gamma channel with pointing errors." IEEE Photonics Journal 11.5 (2019): 1-18.

[74] Ibrahim, Ahmed B., et al. "Structured light transmission under free space jamming: an enhanced mode identification and signal-to-jamming ratio estimation using machine learning." Photonics. Vol. 9. No. 3. MDPI, 2022.

[75] Ragheb, Amr M., Waddah S. Saif, and Saleh A. Alshebeili. "ML-based identification of structured light schemes under free space jamming threats for secure FSO-based applications." Photonics. Vol. 8. No. 4. MDPI, 2021.

[76] Bensalem, Mounir, Sandeep Kumar Singh, and Admela Jukan. "Machine learning techniques to detecting and preventing jammingattacks in optical networks." arXiv preprint arXiv:1902.07537 (2019).

[77] Priyadarshani, Richa, et al. "Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview." arXiv preprint arXiv:2403.19868 (2024).

[78] Yang, Bin, et al. "Friendly cooperation jamming for secrecy in LOS channel." 2012 International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2012.

[79] Lu, Rong-Rong, et al. "Performance analysis and optimization for UAV-based FSO communication systems." Physical Communication 51 (2022): 101594.

[80] Raj, A. Arockia Bazil. "Mono-pulse tracking system for active free space optical communication." Optik 127.19 (2016): 7752-7761.

[81] Shakir, Wafaa, and Ruwaida Abdulkareem. "A survey on physical layer security for FSO communication systems." Proceedings of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies, IMDC-IST 2021, 7-9 September 2021, Sakarya, Turkey. 2022.

[82] Wang, Tyan-Lin, and Ivan B. Djordjevic. "Physical-layer security of a binary data sequence transmitted with Bessel–Gaussian beams over an optical wiretap channel." IEEE Photonics Journal 10.6 (2018): 1-11.

[83] Anthonisamy, Arockia Bazil Raj, and Arputha Vijaya Selvi James. "Formulation of atmospheric optical attenuation model in terms of weather data." Journal of Optics 45 (2016): 120-135.

[84] Jagdale, Atharva Ninad, and AA Bazil Raj. "Model-Free Ber Measurement in Free Space Laser Communication Link." 2021 International Conference on System, Computation, Automation and Networking (ICSCAN). IEEE, 2021.

[85] Arockia Bazil Raj, A., J. Arputha Vijaya Selvi, and S. Durairaj. "Comparison of different models for ground-level atmospheric turbulence strength (Cn 2) prediction with a new model according to local weather data for FSO applications." Applied optics 54.4 (2015): 802-815.

[86] J Soffia Jennifer, Raj, A. Arockia Bazil. “Formulation of Empirical Model for Atmospheric Turbulence Strength (Cn2) Prediction” Conference Proceedings of Kings College of Engineering- 2015

[87] Raj, A. Arockia Bazil, J. Arputha Vijaya Selvi, and S. Raghavan. "Terrestrial free space line of sight optical communication (tfslsoc) using adaptive control steering system with laser beam tracking, aligning and positioning (atp)." 2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC). IEEE, 2010.

[88] Raj, A. Arockia Bazil, and J. Arputha Vijay Selvi. "Lower-order adaptive beam steering system in terrestrial free space point-to-point laser communication using fine tracking sensor." 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies. IEEE, 2011.

[89] Shankaranarayanan, H. "Digital design of fuzzy logic controller for optical beam steering in free space optical communication." 2021 International Conference on System, Computation, Automation and Networking (ICSCAN). IEEE,2021.

[90] Maddegalla, Maheeja, A. Arockia Bazil Raj, and Gurugubelli Syamala Rao. "Beam steering and control algorithm for 5-18ghz transmit/receive module based active planar array." 2020 International Conference on System, Computation, Automation and Networking (ICSCAN). IEEE, 2020.

[91] A Arockia Bazil Raj "Low power and compact RSM and neuralcontroller design for beam wandering mitigation with a horizontal-path propagating Gaussian-beam wave: focused beam case" Free Space Optical Communication.De Gruyter Oldenbourg.- 2015/12/18

[92] A Arockia Bazil Raj 43 "Steering Control system for Laser Beam Tracking" AICTE sponsored Nat. Level Conf. and Sem. Signals, Systems and Communication (SISCOM-2006)

[93] Raj, A. Arockia Bazil, et al. "Low cost beam steering system for FSOC to SMF coupling." IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM-2012). IEEE, 2012.

[94] Raj, A. Arockia Bazil, et al. "Design of cognitive decision making controller for autonomous online adaptive beam steering in free space optical communication system." Wireless Personal Communications 84 (2015): 765- 799.

[95] Arockia Bazil Raj, A., et al. "A direct and neural controller performance study with beam wandering mitigation control in free space optical link." Optical Memory and Neural Networks 23 (2014): 111- 129.

[96] Arockia Bazil Raj, A., and S. Padmavathi. "Statistical analysis of accurate prediction of local atmospheric optical attenuation with a new model according to weather together with beam wandering compensation system: a season-wise experimental investigation." Journal of Modern Optics 63.13 (2016): 1286-1296.

[97] Sharoar Jahan Choyon, A. K. M., and Ruhin Chowdhury. "Performance comparison of free-space optical (FSO) communication link under OOK, BPSK, DPSK, QPSK and 8-PSK modulation formats in the presence of strong atmospheric turbulence." Journal of Optical Communications 44.s1 (2024): s763-s769.

[98] Fadhil, Hilal A., et al. "Optimization of free space optics parameters: An optimum solution for bad weather conditions." Optik 124.19 (2013): 3969-3973.

[99] Ghassemlooy, Zabih, Wasiu Oyewole Popoola, and Erich Leitgeb. "Free-space optical communication using subearrier modulation in gamma-gamma atmospheric turbulence." 2007 9th international conference on transparent optical networks. Vol. 3. IEEE, 2007.

[100] Siegel, Tobias, and Shun-Ping Chen. "Investigations of free space optical communications under real-world atmosphericconditions." Wireless Personal Communications 116.1 (2021): 475-490.

[101] Amirabadi, Mohammad Ali, Mohammad Hossein Kahaei, and S. Alireza Nezamalhosseni. "Low complexity deep learning algorithms for compensating atmospheric turbulence in the free space optical communication system." IET optoelectronics 16.3 (2022):93-105.

[102] Hughes, Richard J., et al. "Quantum cryptography for secure free-space communications." Free-Space Laser Communication Technologies XI. Vol. 3615. SPIE, 1999.

[103] Ikeda, K., et al. "Two-dimensional encryption system for secure free-space optical communication of time-series data streams." Electronics letters 55.13 (2019): 752-754.

[104] Kuang, Randy, and Adrian Chan. "Quantum encryption in phase space with displacement operators." EPJ Quantum Technology 10.1 (2023): 26.

[105] Fuchs, Christian, and Dirk Giggenbach. "Optical Free-Space Communication on Earth and in Space regarding Quantum Cryptography Aspects." Quantum Communication and Quantum Networking: First International Conference, QuantumComm 2009, Naples, Italy, October 26-30, 2009, Revised Selected Papers 1. Springer Berlin Heidelberg, 2010.

[106] El-Meadawy, Shimaa A., et al. "Efficient and secure bit-level chaos security algorithm for orbital angular momentum modulationin free-space optical communications." IEEE Access 9 (2021): 74817-74835.

[107] Hennelly, Bryan M., and J. T. Sheridan. "Optical encryption and the space bandwidth product." Optics communications 247.4-6 (2005): 291-305.

[108] Abd El-Mottaleb, Somia A., et al. "Performance of Cipher Image Transmission in Free Space Optics Under Foggy Weather." IEEE Access (2023).

[109] Abd El-Mottaleb, Somia A., et al. "Performance Enhancement of FSO communication system Under Rainy Weather Environment using a novel encryption technique." IEEE Access (2024).

[110] Durak, Kadir, Naser C. Jam, and Saeid Karamzadeh. "Attack to quantum cryptosystems through RF fingerprints from photon detectors." IEEE Journal of Selected Topics in Quantum Electronics 28.2: Optical Detectors (2021): 1-7.

[111] Ai, Yun, et al. "Comprehensive physical layer security analysis of FSO communications over Málaga channels." IEEE PhotonicsJournal 12.6 (2020): 1-17.

[112] Wang, Jian, et al. "Orbital angular momentum and beyond in free-space optical communications." Nanophotonics 11.4 (2022): 645-680.

[113] Endo, Hiroyuki, et al. "Free-space optical channel estimation for physical layer security." Optics express 24.8 (2016): 8940-8955.

[114] Wang, Tyan-Lin, John A. Gariano, and Ivan B. Djordjevic. "Employing Bessel-Gaussian beams to improve physical-layer security in free-space optical communications." IEEE Photonics Journal 10.5 (2018): 1-13.

[115] Khoshafa, Majid H., et al. "RIS-Assisted Physical Layer Security in Emerging RF and Optical Wireless Communication Systems: A Comprehensive Survey." arXiv preprint arXiv:2403.10412 (2024).

[116] Alhoraibi, Lamia, et al. "Physical layer authentication in wireless networks-based machine learning approaches." Sensors 23.4 (2023): 1814.

[117] Chowdhury, Subhajit Dutta, and Rijuparna Chakraborty. "An Authentication Scheme For Free-Space Laser Communication Using "Fingerprint-Matching"." 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech). IEEE, 2020.

[118] Gu, Wen, Stamatios V. Kartalopoulos, and Pramode K. Verma. "Performance evaluation of EAP-based authentication for proposed integrated mobile WiMAX and FSO access networks." 2011 IEEE Wireless Communications and Networking Conference. IEEE, 2011.

[119] Chattopadhyay, Anish, and Rijuparna Chakrobarty. "A Fabry-Perot Cavity Filtering Scheme for Authentication of Free-Space Laser Communication." 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech). IEEE, 2020.

[120] Abdrabou, Mohammed, and T. Aaron Gulliver. "Physical layer authentication for satellite communication systems using machinelearning." IEEE Open Journal of the Communications Society 3 (2022): 2380-2389.

[121] Abdrabou, Mohammed, and T. Aaron Gulliver. "Authentication for satellite communication systems using physicalcharacteristics." IEEE Open Journal of Vehicular Technology 4 (2022): 48-60.

[122] Qu, Zhiguo, Xinzhu Liu, and Shengyao Wu. "Quantum identity authentication protocol based on three-photon quantum error avoidance code in edge computing." Transactions on Emerging Telecommunications Technologies 33.6 (2022): e3945.

[123] Wang, Ning, et al. "Enhancing the security of free-space optical communications with secret sharing and key agreement." Journalof Optical Communications and Networking 6.12 (2014): 1072-1081.

[124] Wang, Xiaogang, Wen Chen, and Xudong Chen. "Optical information authentication using compressed double-random-phase-encoded images and quick-response codes." Optics express 23.5 (2015): 6239-6253.

[125] Pan, Ziwen, and Ivan B. Djordjevic. "Secret key distillation over satellite-to-satellite free-space optics channel with a limited-sized aperture eavesdropper in the same plane of the legitimate receiver." Optics Express 28.25 (2020): 37129-37148.

[126] Fujiwara, Mikio, et al. "Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link."Optics express 26.15 (2018): 19513-19523.

[127] Khan, Adnan Shahid, et al. "Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based(6-CMAS) cellular network." IEEE Access 11 (2023): 20524-20541.

[128] Pfennigbauer, Martin, et al. Free-space optical quantum key distribution using intersatellite links. na, 2003.

[129] Davidson, Zoe, et al. "AIRQKD: the role of free-space optics quantum key distribution enabling pragmatic secure and scalablecommunications." IEEE Communications Magazine (2024).

[130] Erven, Christopher, et al. "Entangled quantum key distribution over two free-space optical links." Optics express 16.21 (2008):16840-16853.

[131] Weier, Henning, et al. "Free space quantum key distribution: Towards a real life application." Fortschritte der Physik: Progress ofPhysics 54.8-10 (2006): 840-845.

[132] Fürst, M., et al. "Free-space quantum key distribution over 144 km." Advanced Free-Space Optical Communication Techniques/Applications II and Photonic Components/Architectures for Microwave Systems and Displays. Vol. 6399. SPIE, 2006.

[133] Jin, Jeongwan, et al. "Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel."Optics express 27.26 (2019): 37214-37223.

[134] Jain, Adarsh, et al. "Experimental demonstration of free space quantum key distribution system based on the bb84 protocol."2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2020.

[135] Kim, Y -S., Y -C. Jeong, and Y -H. Kim. "Implementation of polarization-coded free-space BB84 quantum key distribution."Laser Physics 18 (2008): 810-814.

[136] Kamran, Muhammad, et al. "Quantum key distribution over free space optic (FSO) channel using higher order Gaussian beam spatial modes." Turkish Journal of Electrical Engineering and Computer Sciences 28.6 (2020): 3335-3351.

[137] Vallone, Giuseppe, et al. "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels."Physical Review A 91.4 (2015): 042320.

[138] Harun, Nur Ziadah, et al. "MQC-MB: Multiphoton Quantum Communication Using Multiple-Beam Concept in Free SpaceOptical Channel." Symmetry 13.1 (2020): 66.

[139] Vergoossen, Tom, et al. "Satellite quantum communications when man-in-the-middle attacks are excluded." Entropy 21.4 (2019):387.

[140] Trinh, Phuc V., et al. "Quantum key distribution over FSO: Current development and future perspectives." 2018 Progress inElectromagnetics Research Symposium (PIERS-Toyama). IEEE, 2018.

[141] Amirabadi, M. A. "A survey on machine learning for optical communication [machine learning view]." arXiv preprintarXiv:1909.05148 (2019).

[142] Bensalem, Mounir, Sandeep Kumar Singh, and Admela Jukan. "Machine learning techniques to detecting and preventingjamming attacks in optical networks." arXiv preprint arXiv:1902.07537 (2019).

[143] Trinh, Phuc V., et al. "Statistical verifications and deep-learning predictions for satellite-to-ground quantum atmosphericchannels." Communications Physics 5.1 (2022): 225.

[144] Argyris, Apostolos, Julián Bueno, and Ingo Fischer. "Photonic machine learning implementation for signal recovery in opticalcommunications." Scientific reports 8.1 (2018): 8487.

[145] Zhu, Xiaoming, and Joseph M. Kahn. "Free-space optical communication through atmospheric turbulence channels." IEEETransactions on communications 50.8 (2002): 1293-1300.

[146] Al-Mohammed, Hasan Abbas, et al. "Machine learning techniques for detecting attackers during quantum key distribution in IoTnetworks with application to railway scenarios." IEEE Access 9 (2021): 136994-137004.

[147] Long, Nathan K., Robert Malaney, and Kenneth J. Grant. "A survey of machine learning assisted continuous-variable quantumkey distribution." Information 14.10 (2023): 553.

[148] Ozay, Mete, et al. "Machine learning methods for attack detection in the smart grid." IEEE transactions on neural networks andlearning systems 27.8 (2015): 1773-1786.

[149] Natalino, Carlos, et al. "Experimental study of machine-learning-based detection and identification of physical-layer attacks inoptical networks." Journal of Lightwave Technology 37.16 (2019): 4173-4182.

[150] Musumeci, Francesco, et al. "An overview on application of machine learning techniques in optical networks." IEEECommunications Surveys & Tutorials 21.2 (2018): 1383-1408.

[151] Abadi, Mojtaba Mansour, et al. "Dual purpose antenna for hybrid free space optics/RF communication systems." Journal ofLightwave Technology 34.14 (2016): 3432-3439.

[152] Vangala, Sarma, and Hossein Pishro-Nik. "Optimal hybrid RF-wireless optical communication for maximum efficiency andreliability." 2007 41st Annual Conference on Information Sciences and Systems. IEEE, 2007.

[153] Magidi, Simbarashe, and A. Jabeena. "Free space optics, channel models and hybrid modulation schemes: A review." WirelessPersonal Communications 119.4 (2021): 2951-2974.

[154] Aboelala, Omar, It Ee Lee, and Gwo Chin Chung. "A survey of hybrid free space optics (FSO) communication networks toachieve 5G connectivity for backhauling." Entropy 24.11 (2022): 1573.

[155] Wang, Dawei, et al. "Privacy preserving with adaptive link selection for hybrid radio-frequency and free space optical networks."Optics express 27.3 (2019): 3121-3135.

[156] Ai, Yun, et al. "Physical layer security of hybrid satellite-FSO cooperative systems." IEEE Photonics Journal 11.1 (2019): 1-14.